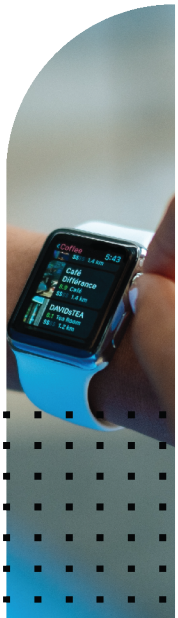
New Features Guide

FortiAnalyzer 7.0.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

July 15, 2021
FortiAnalyzer 7.0.0 New Features Guide
05-700-698019-20210715

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-04-22	Initial release of FortiAnalyzer 7.0.0.
2021-04-23	Added Data sources tuning on page 42.
2021-04-29	Updated Shadow IT Monitoring Service on page 39.
2021-04-30	Added: • FortiAnalyzer Federation on page 110 • Admins can use a SAML SSO FortiCloud account to log in to FortiAnalyzer on page 89
2021-05-10	Added CSF support for multiple VDOMs on page 117.
2021-05-26	Added Improved secure SD-WAN monitor on page 11.
2021-07-15	Added FortiAnalyzer HA graceful upgrade on page 81.
2021-07-15	Initial release of FortiAnalyzer 7.0.1.

FortiAnalyzer 7.0.0 New Features Guide

This document describes the new features added to FortiAnalyzer 7.0.0. The FortiAnalyzer new features are organized into the following categories:

Device Manager

This section lists the new features added to FortiAnalyzer for the device manager:

Device and Groups

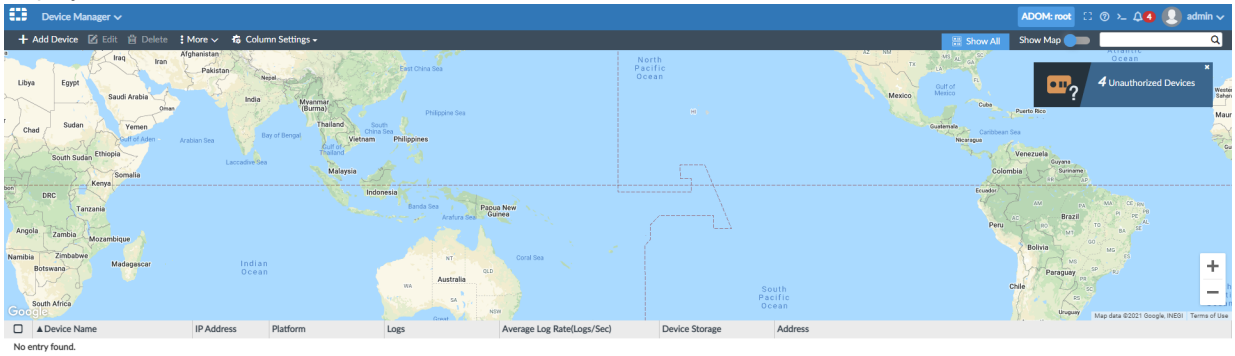
This section lists the new features added to FortiAnalyzer for devices and groups:

World map added to the Device Manager

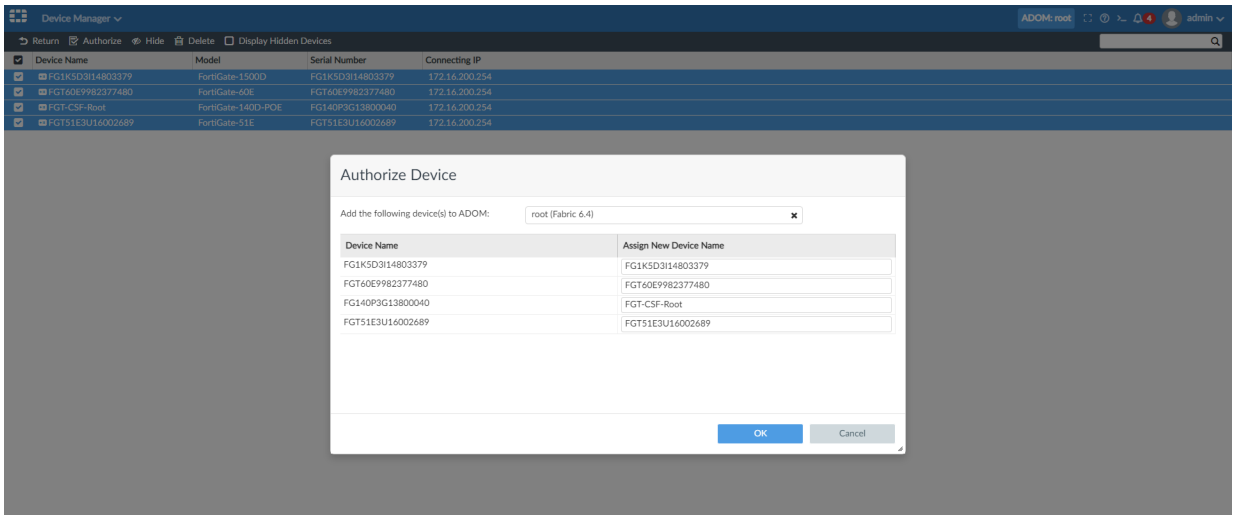
An enhancement to the Device Manager page which shows the locations of the registered device in a world map.

To view the world map in Device Manager:

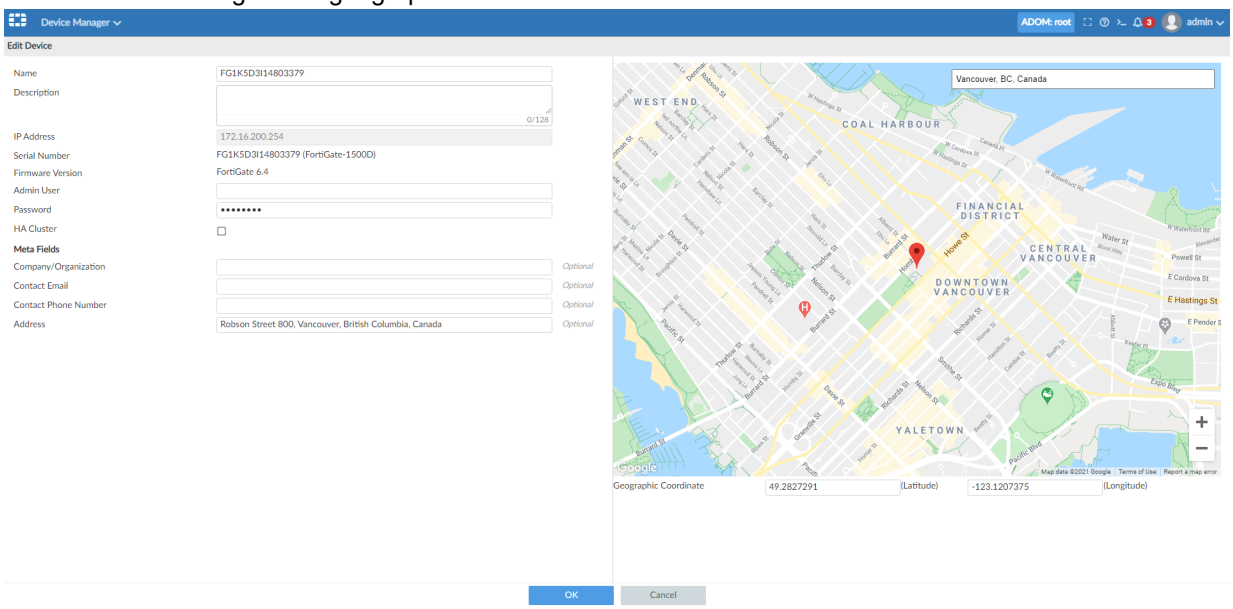
1. Go to Device Manager in the FortiAnalyzer GUI. By default, the *Show Map* toggle is enabled and the map is displayed.



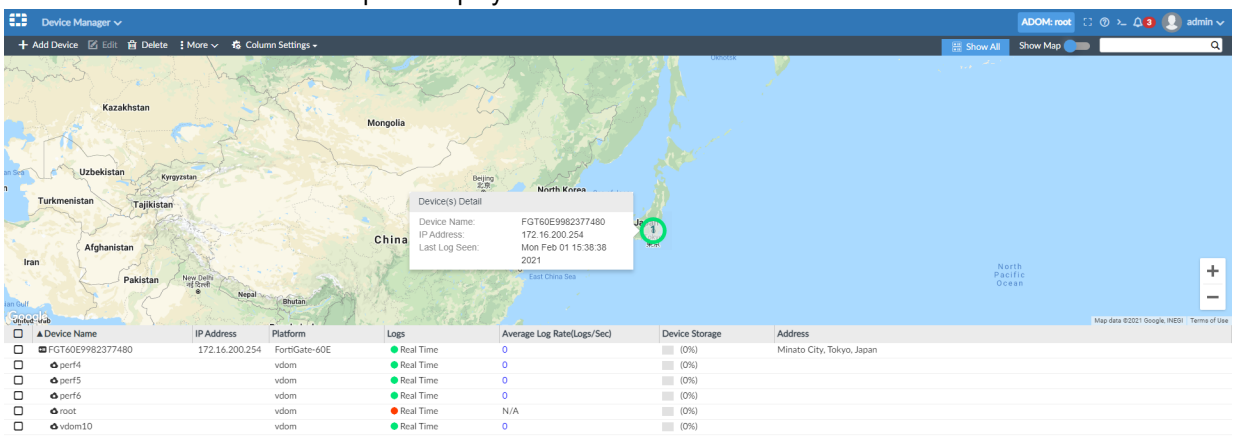
When there are unregistered devices, a small *Unauthorized Devices* window is displayed on the map. Click *Unauthorized Devices* to view all unauthorized devices in a table. Administrators are able to authorize devices from this view. Click *Return* to view authorized devices and the map.



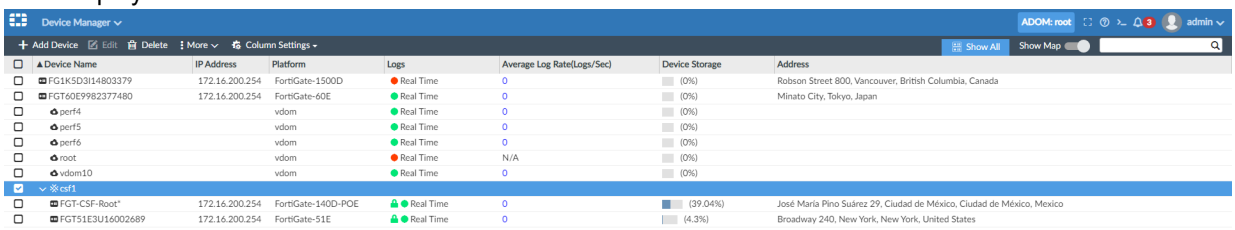
2. Edit a device to configure the geographic coordinates for each device.



Configured device locations are displayed on the world map. You can zoom in or out on the world map. Only the devices that are visible in the map are displayed in the table below.



3. To disable the world map, set the Show Map toggle to the off position. When the world map is disabled, the device table displays all authorized devices.

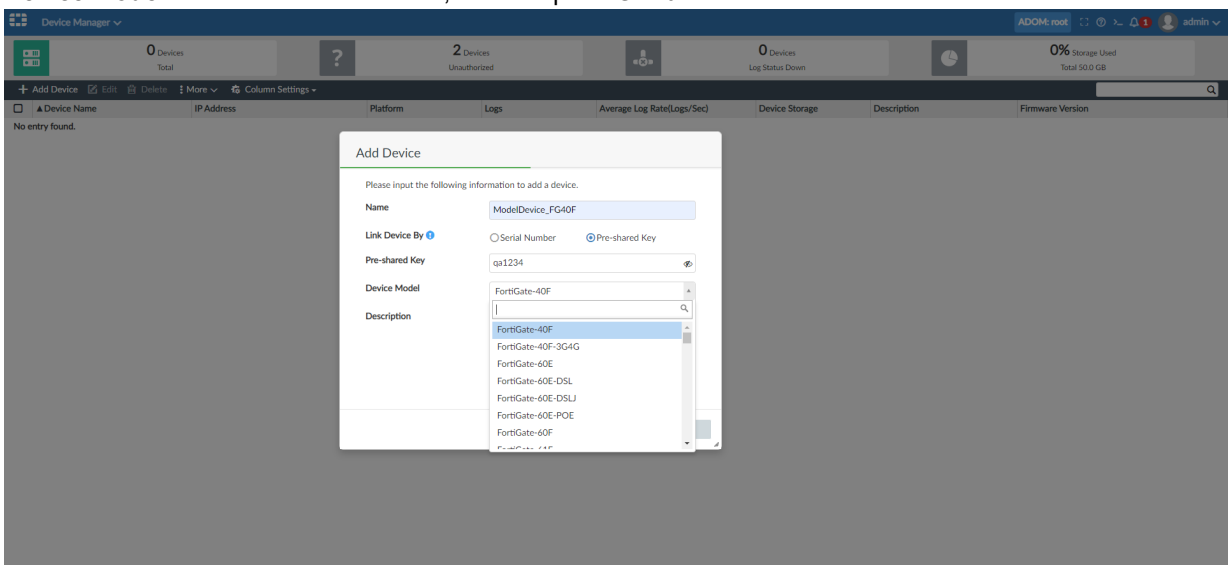


Model device support for central logging

FortiAnalyzer includes the option to add a device as a model device in *Device Manager* and auto-link the device using a pre-shared key when the real device connects to FortiAnalyzer.

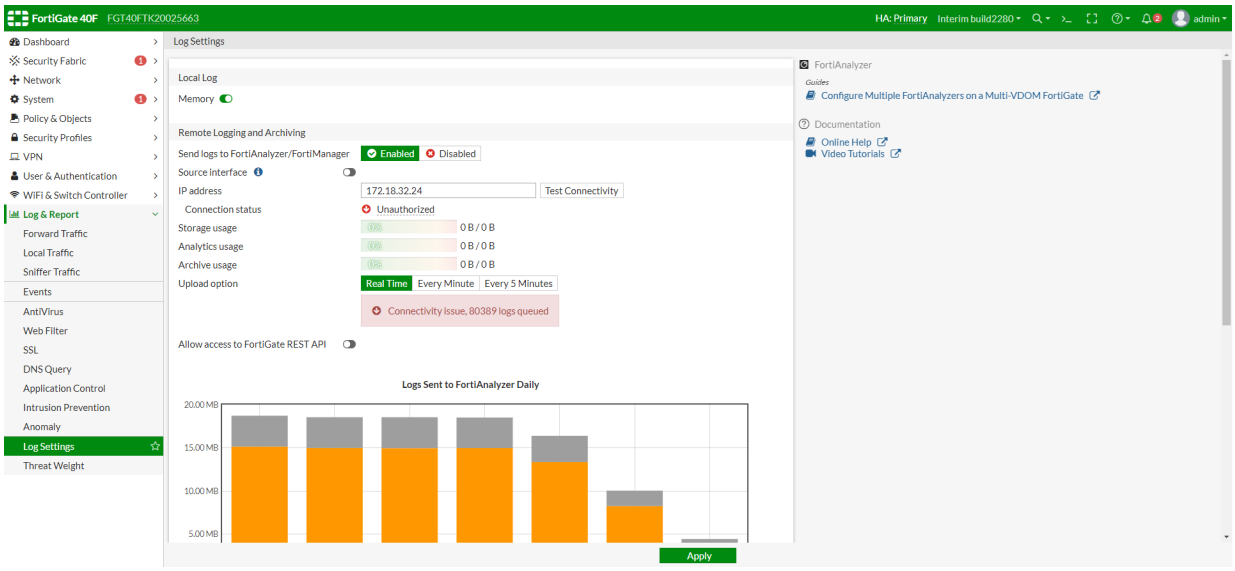
To add devices using a pre-shared key:

1. On FortiAnalyzer, go to the *Device Manager*, and click *Add Device*.
2. Under *Link Device By* select *Pre-shared Key*, configure the settings for your device, and click *Next*.
   a. **Name**: Enter a name for the device, for example, *ModelDevice_FG40F*.
   b. **Pre-shared Key**: Enter a pre-shared key, for example: *qa1234*.
   c. **Device Model**: Select the device model, for example: *FGT40F*.



The device is added successfully but is not yet authorized.

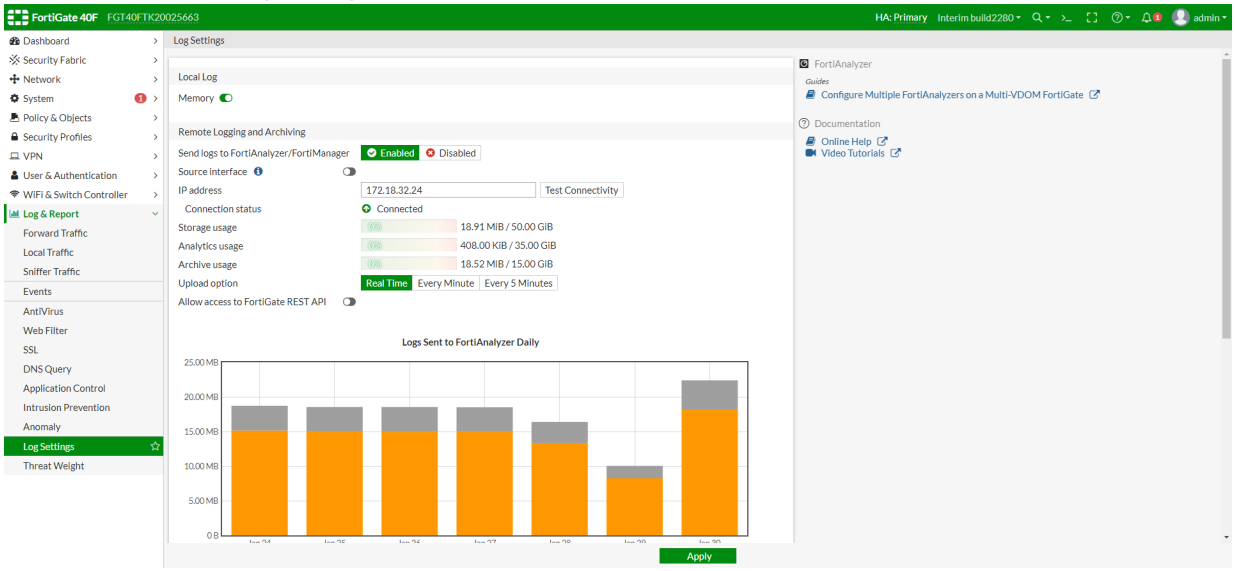
3. On the FortiGate, go to *Log Settings* to configure the FortiAnalyzer. At this time, the connection status is unauthorized.



4. In the FortiGate CLI, configure the pre-shared key to match the one configured on the FortiAnalyzer, for example qa1234.

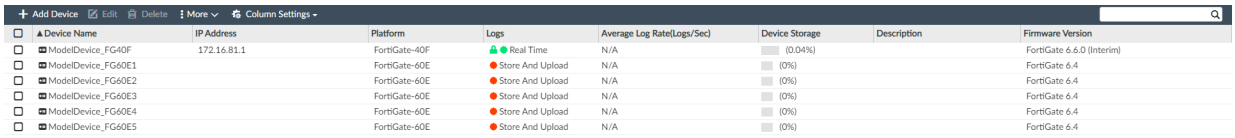
```
config log fortianalyzer setting
set preshared-key <your pre-shared key>
```

5. On FortiAnalyzer, go to the *Device Manager* and refresh the table. The FortiGate device is recognized and is automatically authorized as a registered device.
6. On FortiGate, check *Log Settings* to confirm the connection status is *Connected*.

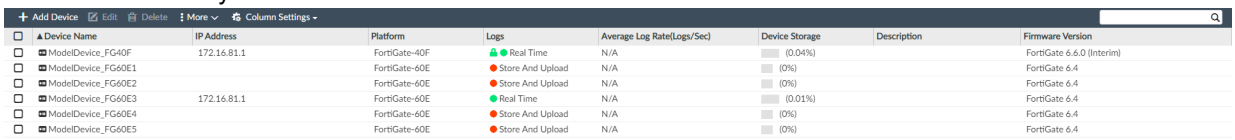


To add multiple devices using the same FortiGate platform:

1. On FortiAnalyzer, go to the *Device Manager* and configure multiple model devices using the same FortiGate platform. Each configured device must have a unique pre-shared key. In this example, five devices are configured.



2. When a corresponding FortiGate device is configured to send logs to the FortiAnalyzer, and it is configured with a pre-shared key matching one of the five configured in FortiAnalyzer, it is automatically authorized as a registered device on FortiAnalyzer.



SD-WAN

This section lists the new features added to FortiAnalyzer for SD-WAN:

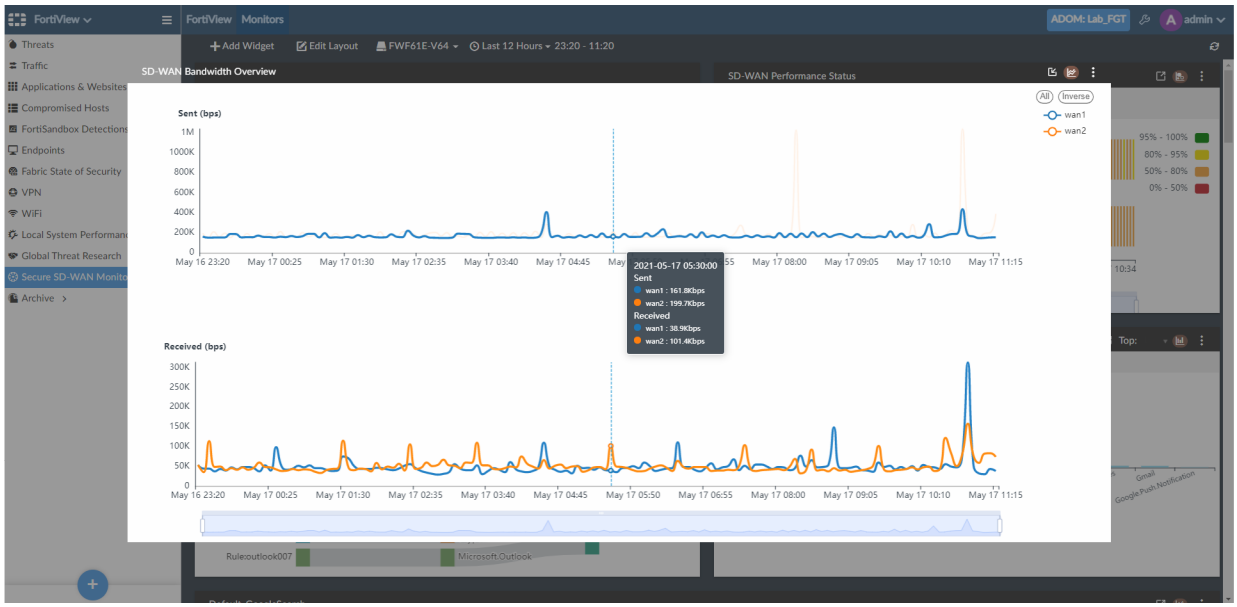
- Improved secure SD-WAN monitor on page 11

Improved secure SD-WAN monitor

This is an enhancement to the existing Secure SD-WAN Monitor dashboard by providing more widgets and detailed information.

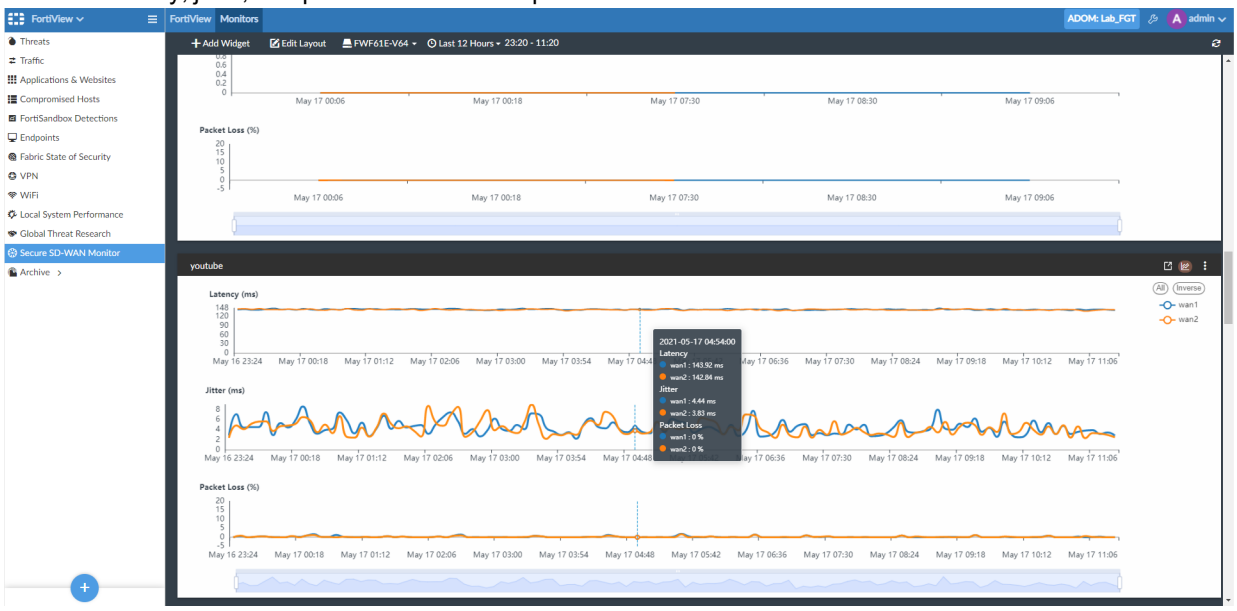
To view the secure SD-WAN monitor enhancements:

1. Go to *FortiView* > *Monitors* > *Secure SD-WAN Monitor*.
   A new widget called *SD-WAN Bandwidth Overview* has been added which displays a line chart of the sent/received rate (bps) in the selected time period for SD-WAN members interfaces. In this widget, users can select or deselect member interfaces and mouse over the line chart to view the sent/received rate in a tooltip for the selected interfaces.

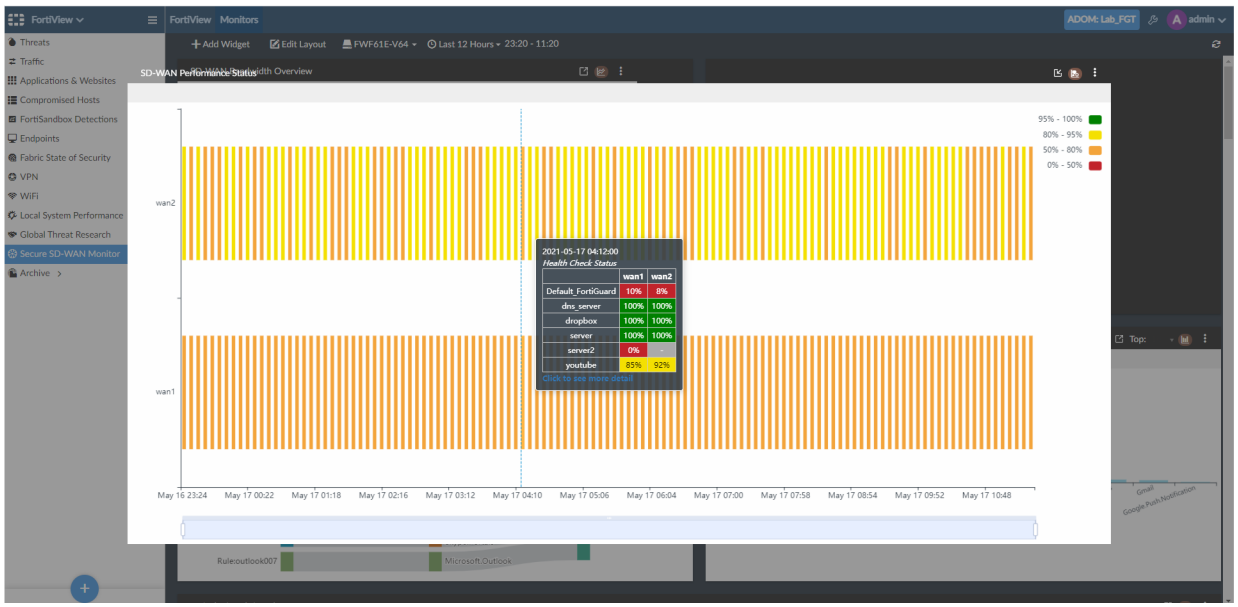


The *Latency*, *Jitter*, and *Packet Loss* widgets have been replaced with the new *Health Check Status* widget. This widget dynamically creates a child-widget for each health check where a line chart of latency, jitter, and packet loss in the selected time period for SD-WAN interfaces is displayed.

In each *Health Check Status* widget, users can select/deselect member interfaces and mouse over line charts to view the latency, jitter, and packet loss in a tooltip for the selected interface.

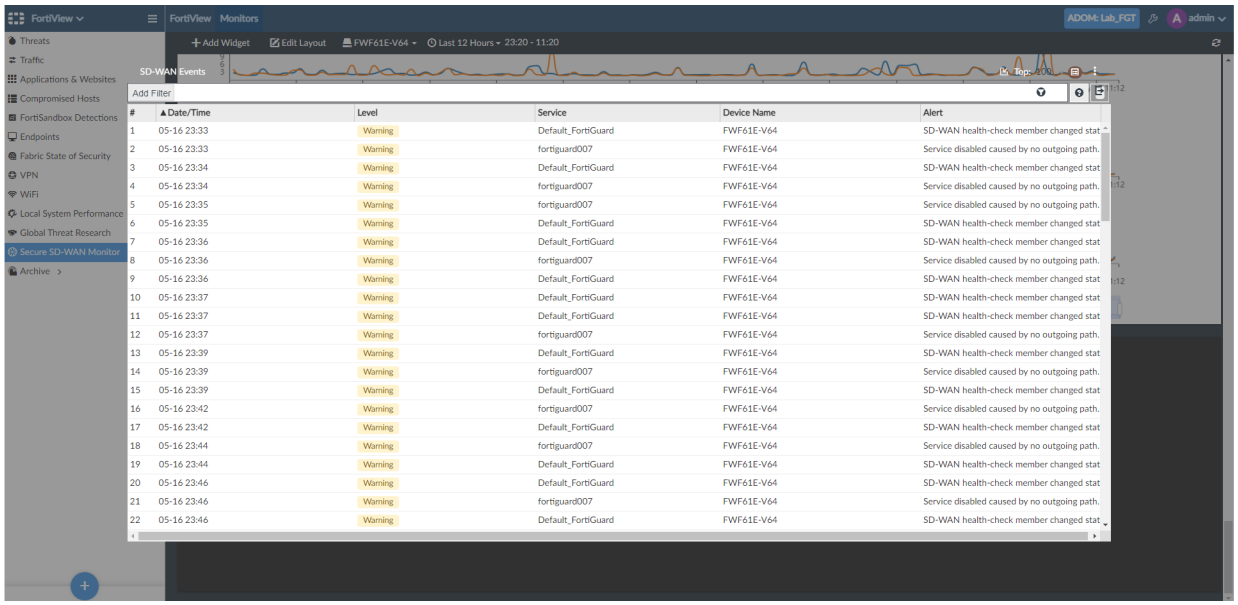


In the *SD-WAN Performance Status* widget, mousing over the scatter chart displays the status for health checks and member interface in a tooltip. The colors (red, orange, yellow, and green) indicate the different percentage of a member's interface or health check.



In the *SD-WAN Performance Status* widget, click on a scatter chart to view additional details.

The *SD-WAN High and Critical Events* widget has been replaced with the new *SD-WAN Events* widget. This widget displays a table chart for SD-WAN event logs which have a level higher than notice (warning, error, etc.) within the selected time period.


FortiView
Monitors
ADOM: Lab_FGT
admin
Threats
Traffic
Applications & Websites
Compromised Hosts
FortiSandbox Detections
Endpoints
Fabric State of Security
VPN
WiFi
Local System Performance
Global Threat Research
Secure SD-WAN Monitor
Archive
Add Widget
Edit Layout
FWF61E-V64
Last 12 Hours
23:20 - 11:20
SD-WAN Events
Add Filter
| Date/Time | Level | Service | Device Name | Alert
1 | 05-16 23:33 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
2 | 05-16 23:33 | Warning | fortiguard007 | FWF61E-V64 | Service disabled caused by no outgoing path.
3 | 05-16 23:34 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
4 | 05-16 23:34 | Warning | fortiguard007 | FWF61E-V64 | Service disabled caused by no outgoing path.
5 | 05-16 23:35 | Warning | fortiguard007 | FWF61E-V64 | Service disabled caused by no outgoing path.
6 | 05-16 23:35 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
7 | 05-16 23:36 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
8 | 05-16 23:36 | Warning | fortiguard007 | FWF61E-V64 | Service disabled caused by no outgoing path.
9 | 05-16 23:36 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
10 | 05-16 23:37 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
11 | 05-16 23:37 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
12 | 05-16 23:37 | Warning | fortiguard007 | FWF61E-V64 | Service disabled caused by no outgoing path.
13 | 05-16 23:39 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
14 | 05-16 23:39 | Warning | fortiguard007 | FWF61E-V64 | Service disabled caused by no outgoing path.
15 | 05-16 23:39 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
16 | 05-16 23:42 | Warning | fortiguard007 | FWF61E-V64 | Service disabled caused by no outgoing path.
17 | 05-16 23:42 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
18 | 05-16 23:44 | Warning | fortiguard007 | FWF61E-V64 | Service disabled caused by no outgoing path.
19 | 05-16 23:44 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
20 | 05-16 23:46 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat
21 | 05-16 23:46 | Warning | fortiguard007 | FWF61E-V64 | Service disabled caused by no outgoing path.
22 | 05-16 23:46 | Warning | Default_FortiGuard | FWF61E-V64 | SD-WAN health-check member changed stat

Security Operations (SOC)

This section lists the new features added to FortiAnalyzer for security operations (SOC):

SOC automation

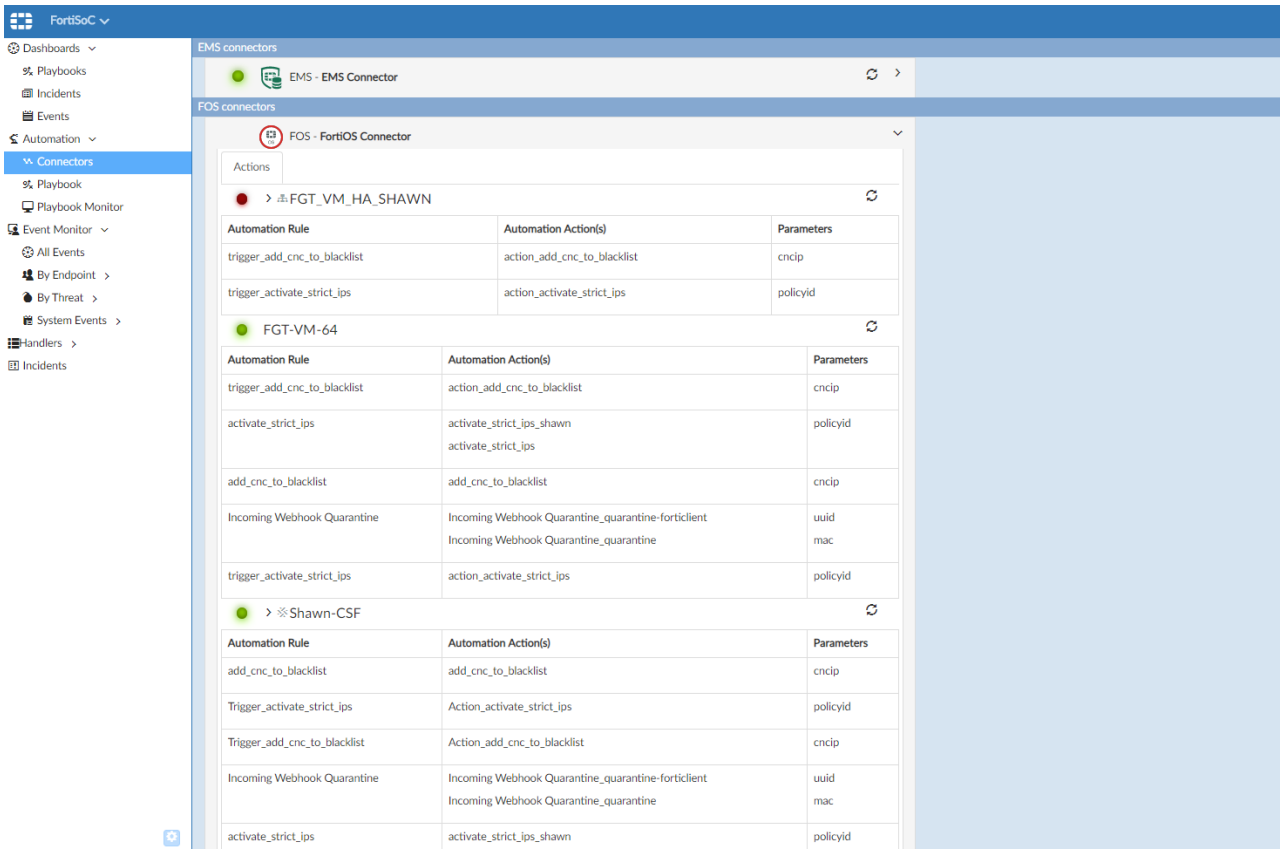
This section lists the new features added to FortiAnalyzer for SOC automation:

FortiOS connector health check

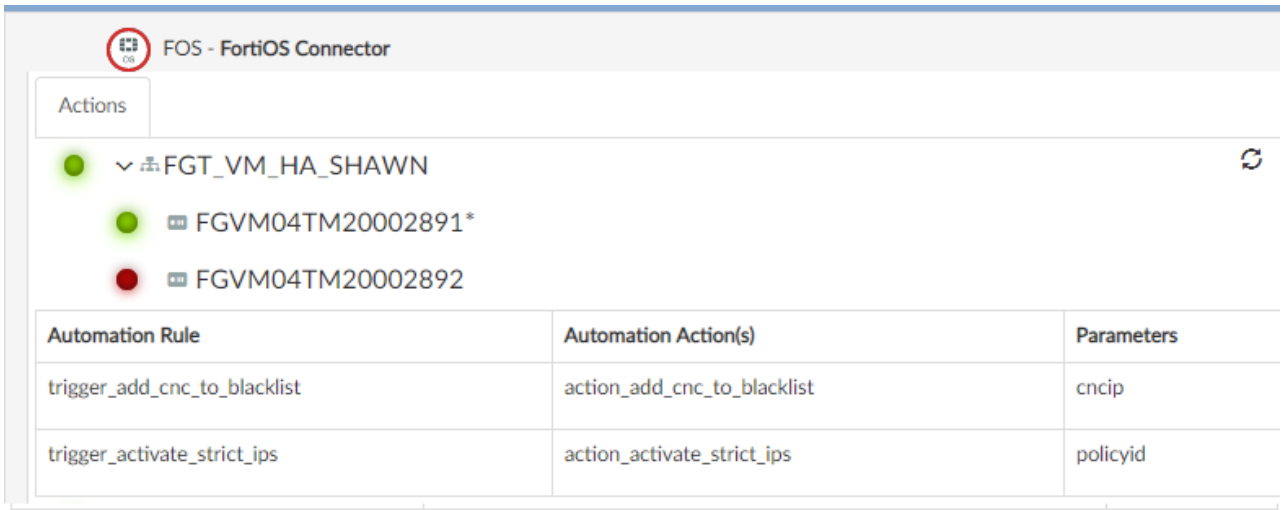
This enhanced feature provides visibility on the FortiOS connectors status.

To view the status of FortiOS connectors:

1. Go to *FortiSoC* > *Automation* > *Connectors*, and click the FortiOS connector to expand the list and display all FortiGate devices.



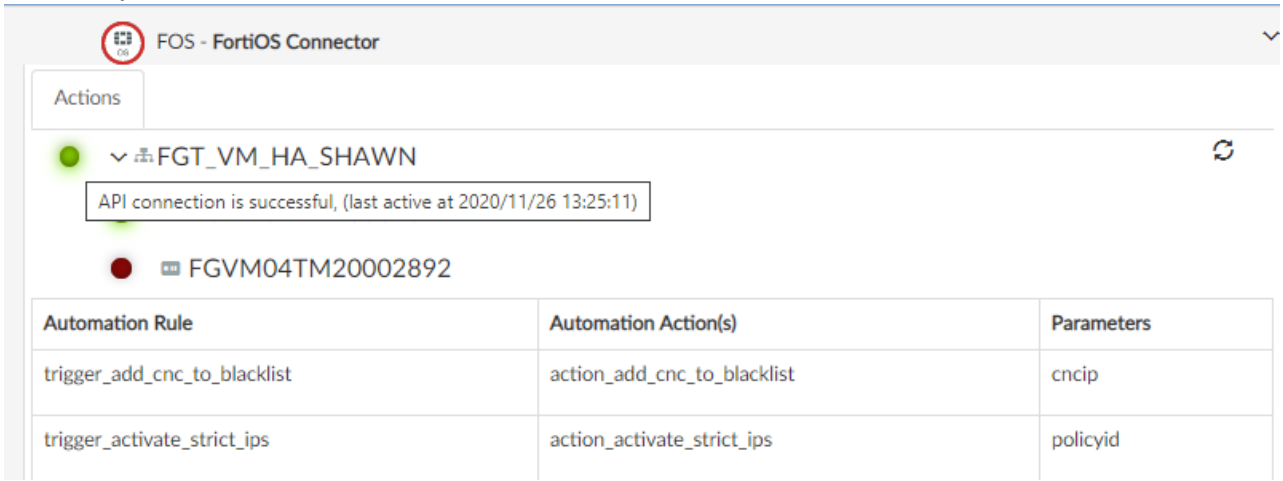
Devices are organized by standalone, Cooperative Security Fabric (CSF), and high availability (HA). Clicking a CSF or HA grouping will expand the list to display all FortiGate members.



Automation Rule	Automation Action(s)	Parameters
trigger_add_cnc_to_blacklist	action_add_cnc_to_blacklist	cncip
trigger_activate_strict_ips	action_activate_strict_ips	policyid

Automation Rule	Automation Action(s)	Parameters
add_cnc_to_blacklist	add_cnc_to_blacklist	cncip
Trigger_activate_strict_ips	Action_activate_strict_ips	policyid
Trigger_add_cnc_to_blacklist	Action_add_cnc_to_blacklist	cncip
Incoming Webhook Quarantine	Incoming Webhook Quarantine_quarantine-forticlient Incoming Webhook Quarantine_quarantine	uuid mac
activate_strict_ips	activate_strict_ips_shawn activate_strict_ips	policyid

Status icons in green indicate the API connection is up. Status icons in red indicate the API connection is down. You can hover your mouse over a status icon to see the last active time.



Automation Rule	Automation Action(s)	Parameters
trigger_add_cnc_to_blacklist	action_add_cnc_to_blacklist	cncip
trigger_activate_strict_ips	action_activate_strict_ips	policyid

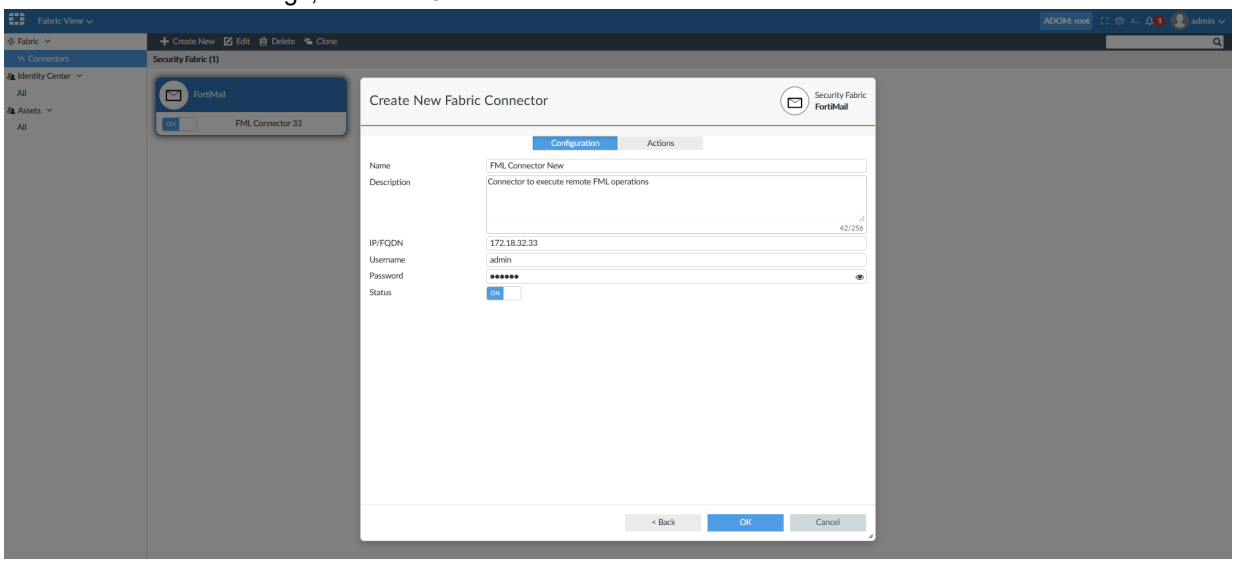
Click the refresh icon to get an updated connector status.

Attach FortiMail connector actions to incidents

This feature will help users to see the result of FortiMail playbook actions in the incident analysis page. Information can be found within the *Indicators* tab of the incident analysis page once added.

To use the action in a FortiSoC playbook:

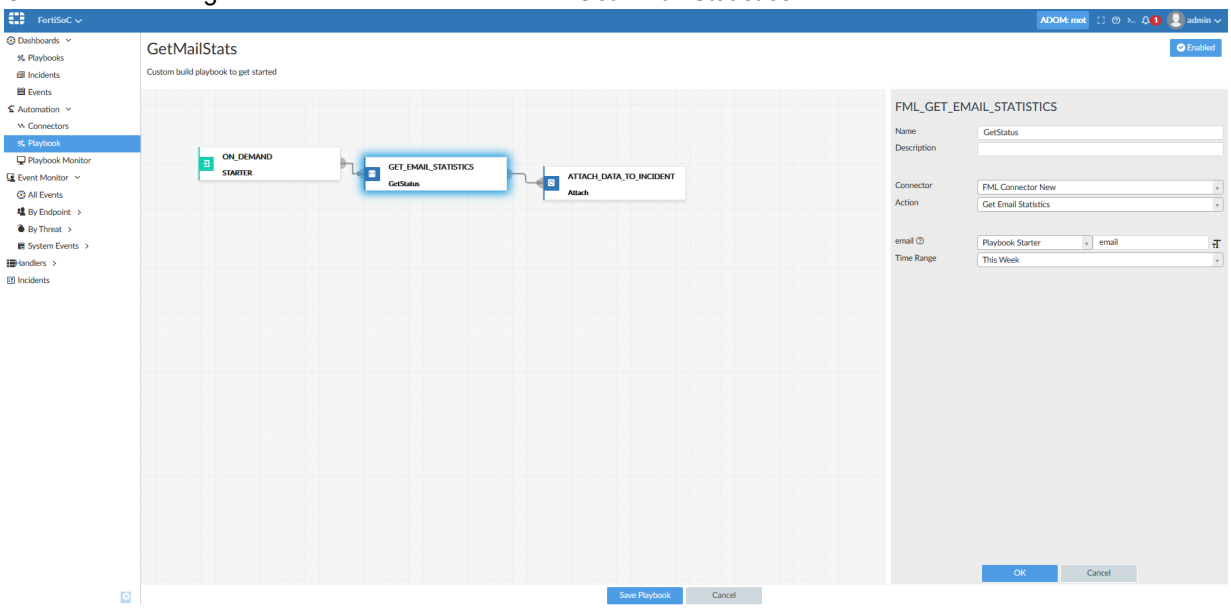
1. Go to *Fabric View*. Click *Create New* and choose *FortiMail* under the *Security Fabric* category. Configure the FortiMail connector settings, and click *OK*.



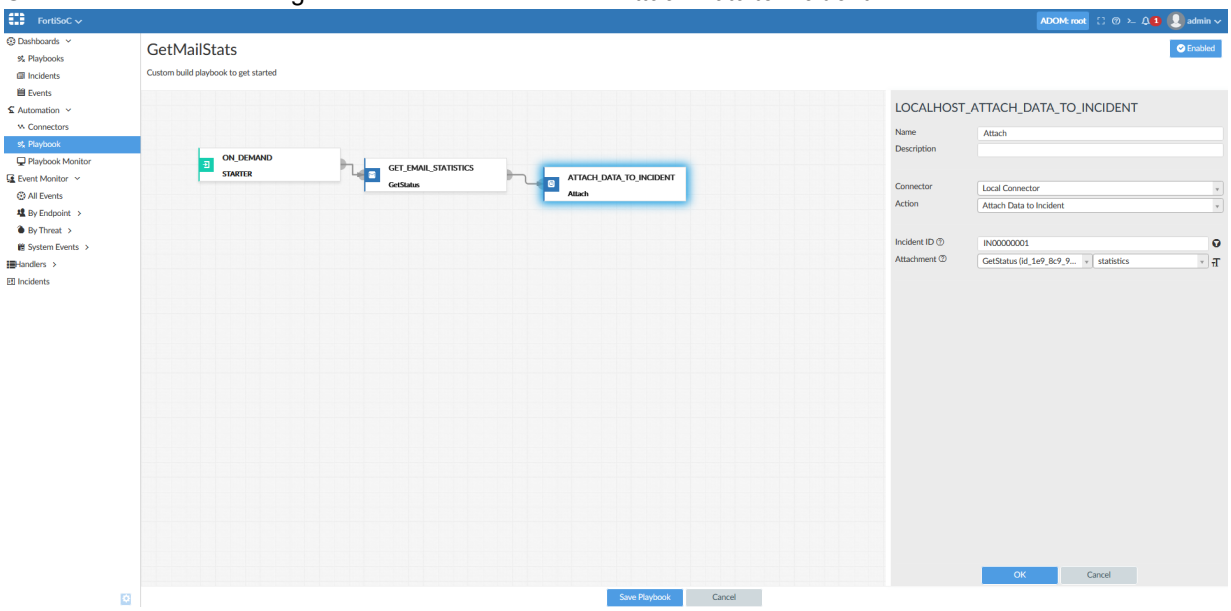
2. Create a playbook to get email statistics and attach the data to an incident.
   Go to *FortiSoC* > *Automation* > *Playbook*, and create a new playbook from scratch. In this example, the playbook is called *GetMailStats*.

a. Select the *On_Demand* trigger as the starter.

b. Create a task using the FortiMail connector with the *Get Email Statistics* action.



c. Create a second task using the local connector with the *Attach Data to Incident* action.

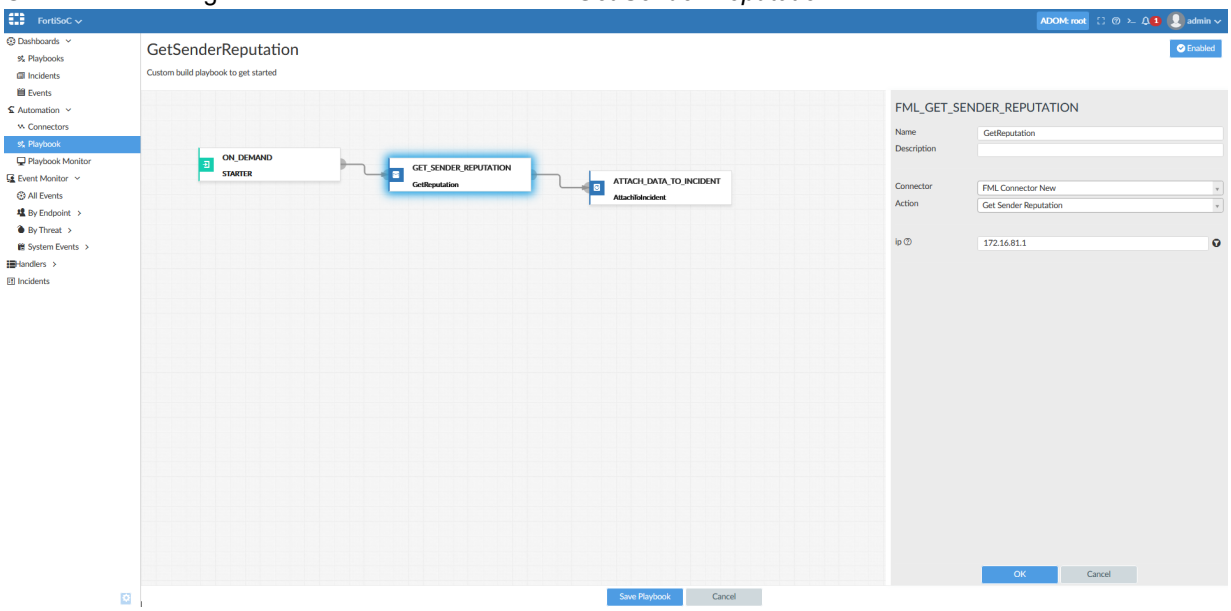


d. Click *OK* to save the playbook.

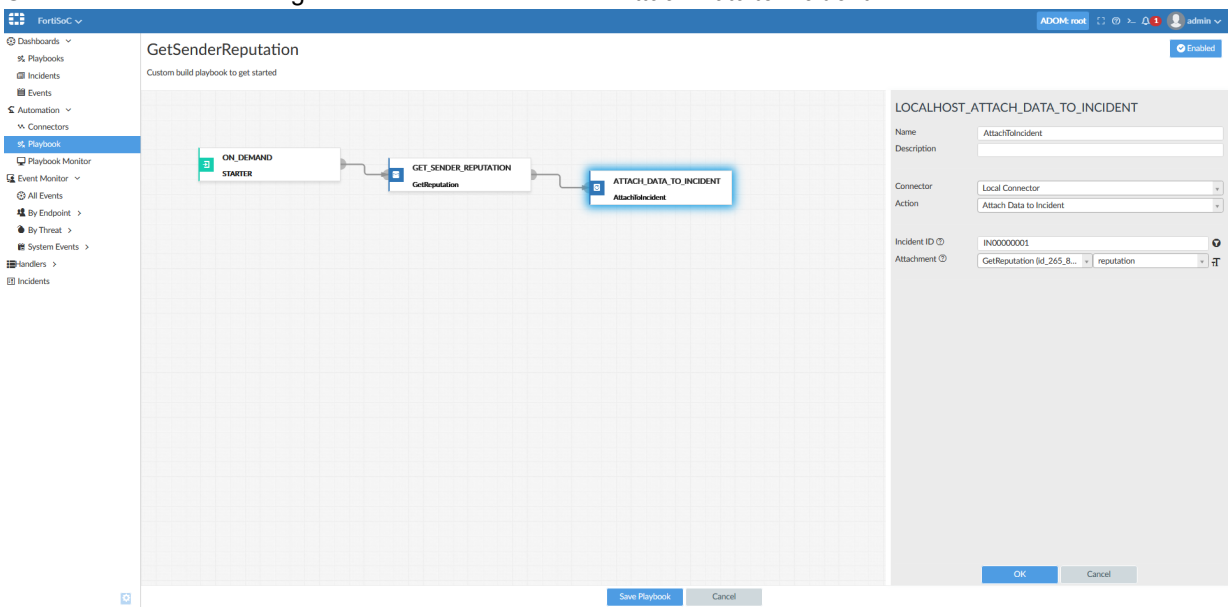
3. Create a second playbook to get the sender reputation and attach the data to an incident. In this example, the playbook is called *GetSenderReputation*.

a. Select the *On_Demand* trigger as the starter.

b. Create a task using the FortiMail connecter with the *Get Sender Reputation* action.

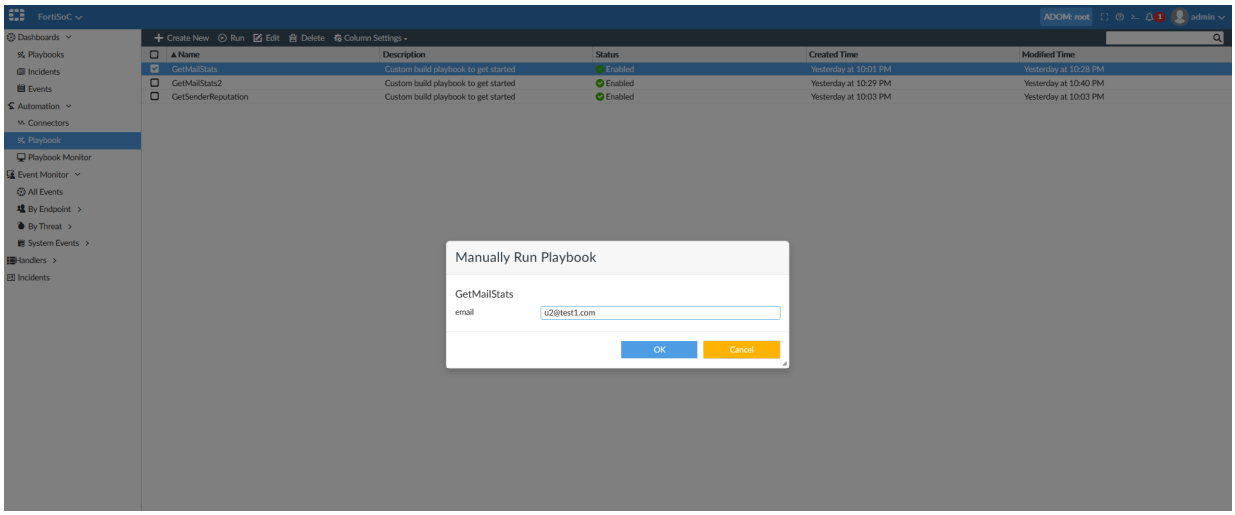


c. Create a second task using the local connector with the *Attach Data to Incident* action.

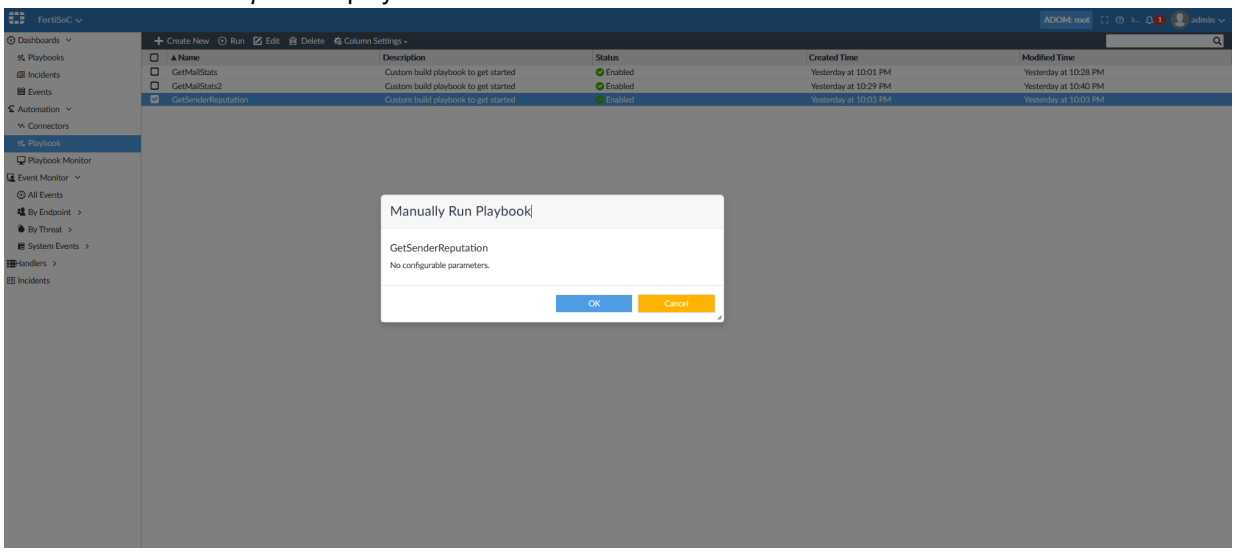


d. Click *OK* to save the playbook.

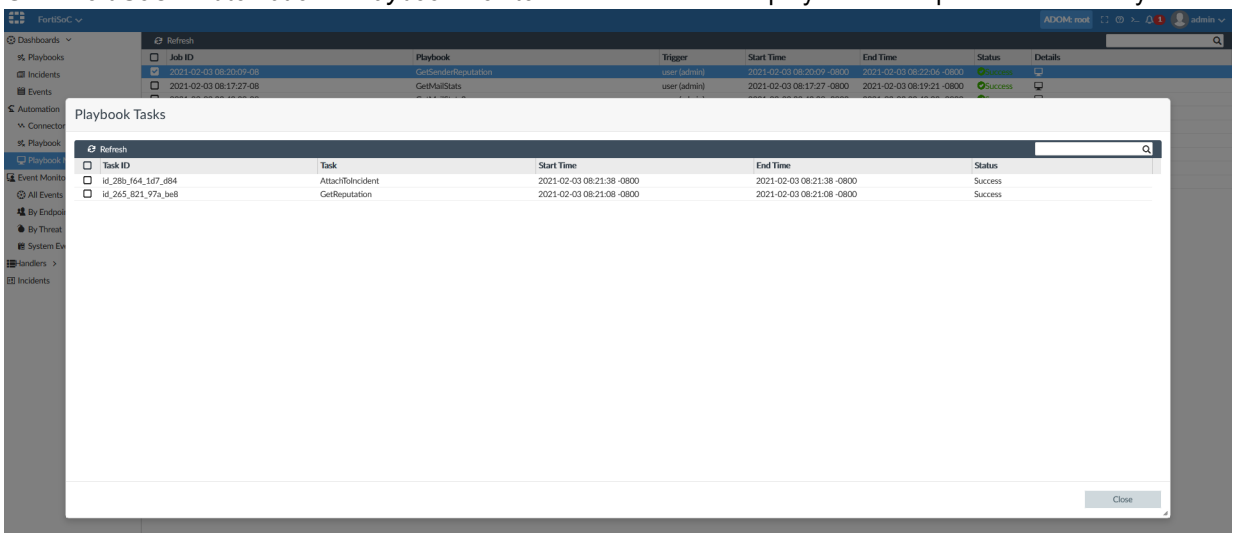
4. Run the *GetMailStats* playbook to retrieve statistics for the provided email address. This example uses `u2@test1.com`.



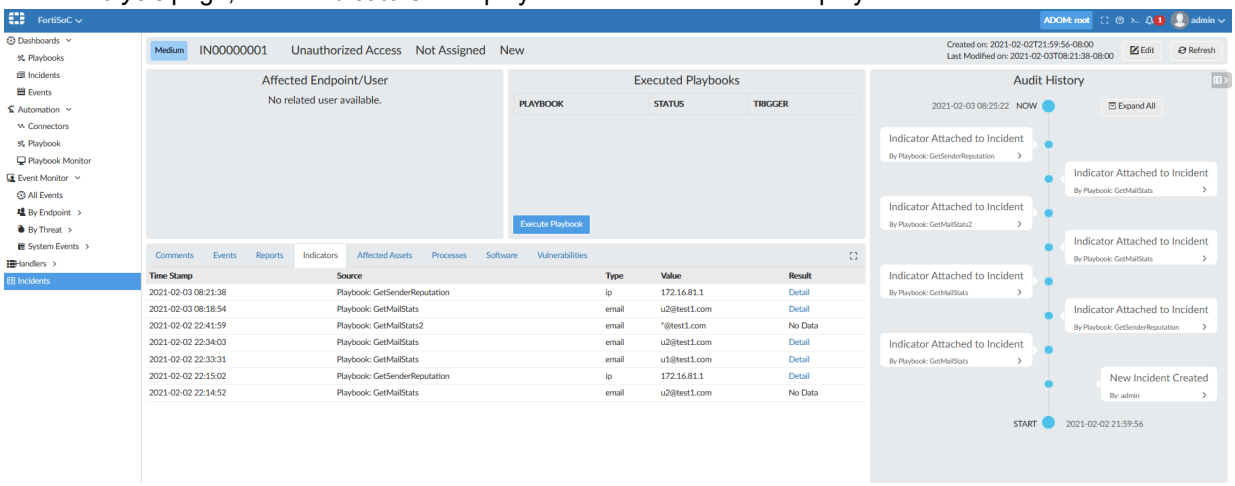
5. Run the *GetSenderReputation* playbook.



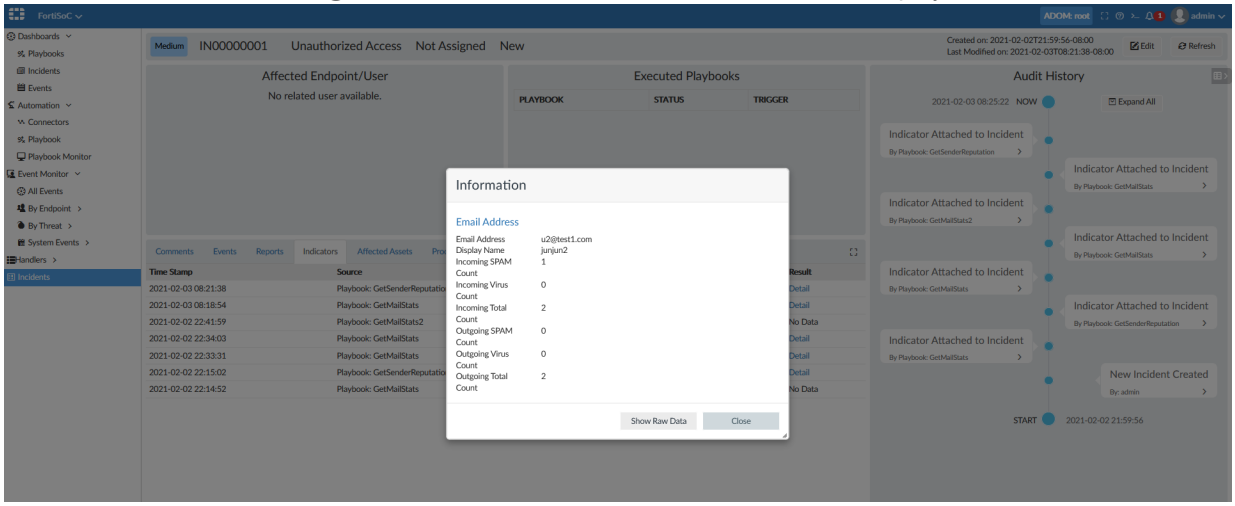
6. Go to *FortiSoC* > *Automation* > *Playbook Monitor* to confirm that both playbooks completed successfully.



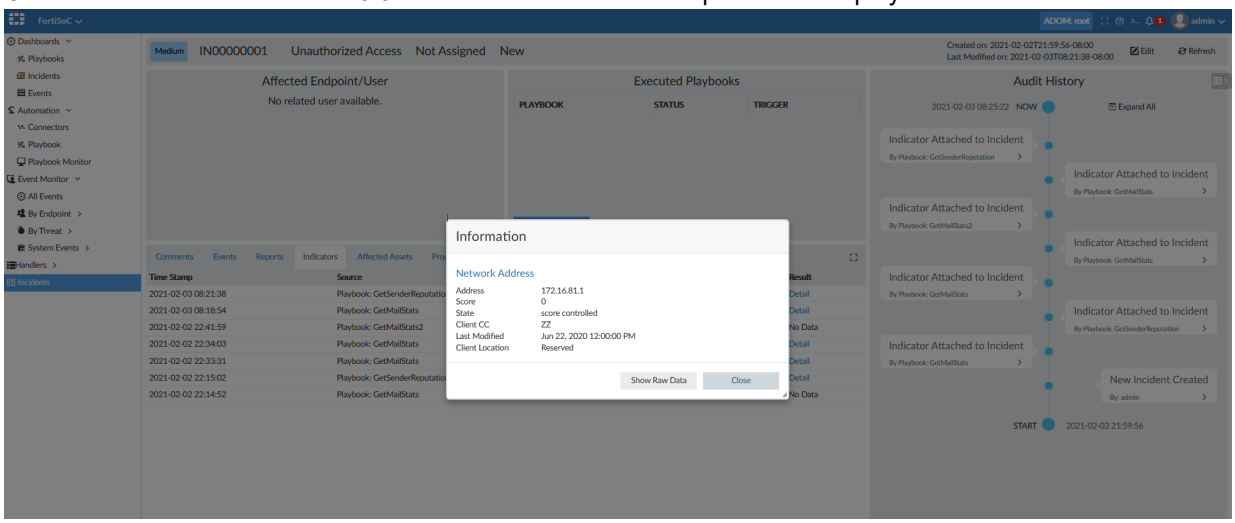
7. Go to *FortiSoC* > *Incidents*. Right-click on the selected incident and select *Analysis*.
In the *Analysis* page, select *Indicators*. The playbook action results are displayed.



Click on the details for the u2@test1 email address. The detailed statistics are displayed.



Click on the details for the 172.16.81.1 address. The detailed reputation is displayed.

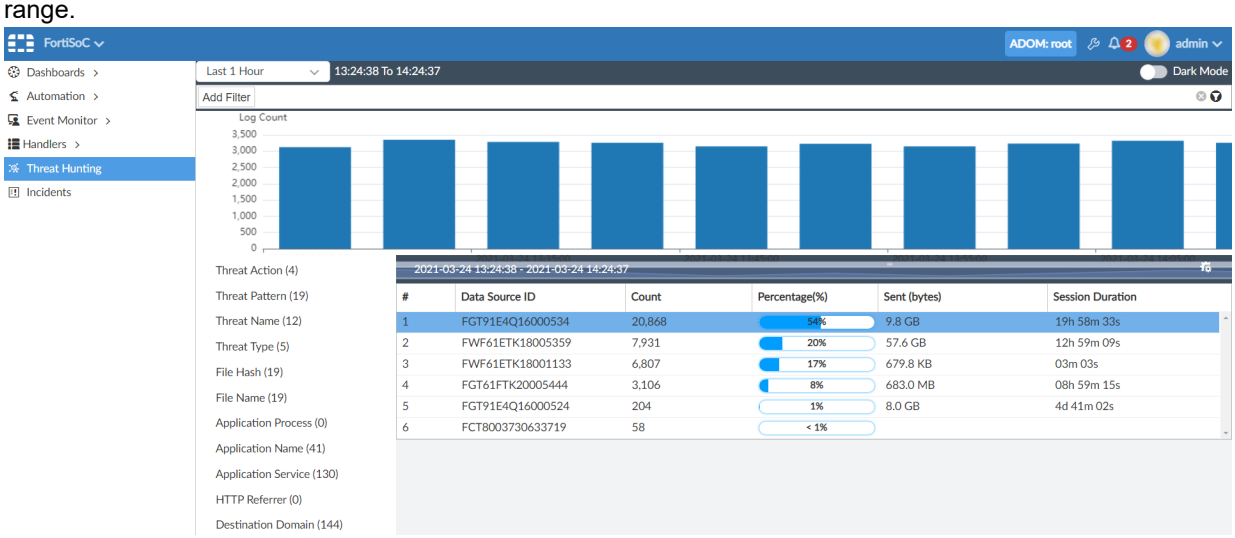


SIEM correlation and analysis

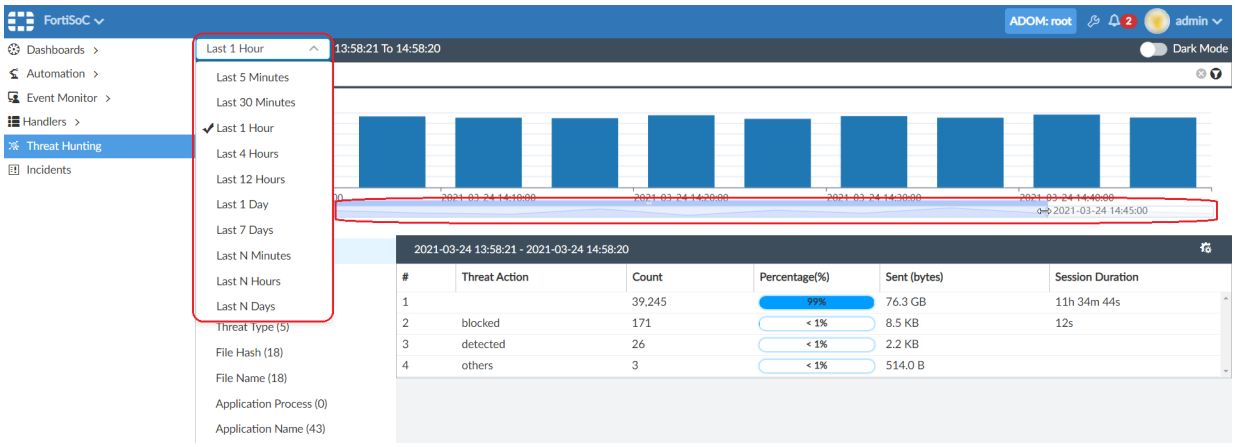
Expand the built-in SIEM framework for automated correlation and analysis using the normalized log fields that are critical for SOC threat hunting. Data is aggregated, correlated across these interesting log fields, and organized in a digestible format ready for SOC to consume. Global filters can be applied on the fly to help the SOC quickly zero into the interesting timeline, endpoint events, and suspicious activities, identify anomalies and behavior patterns and uncover hidden threats.

To view the Threat Hunting dashboard:

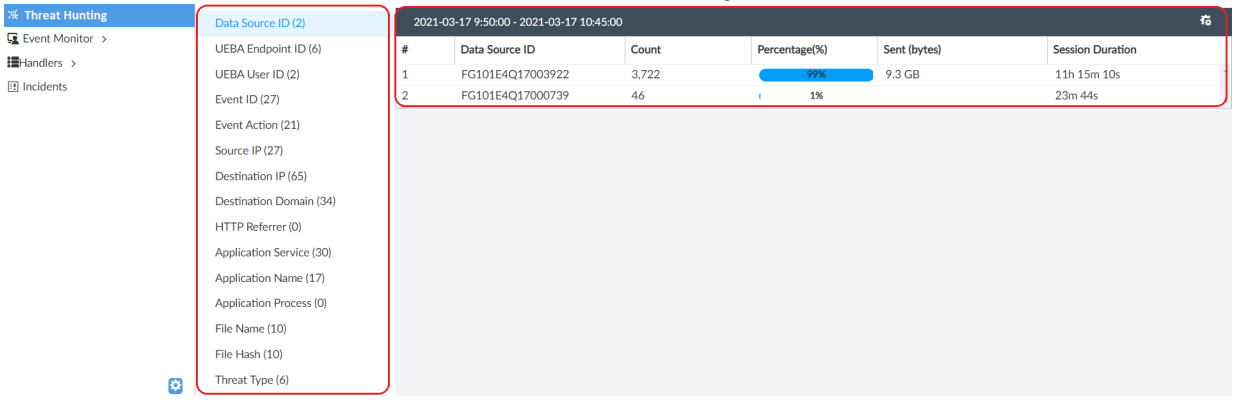
1. Go to *FortiSoC* > *Threat Hunting*.
   The *Threat Hunting* dashboard is displayed. This dashboard provides fast searching (drilldown) with cached data on fields of interest based on the SIEM database and includes a graphical chart for Log Count during the specified time range.



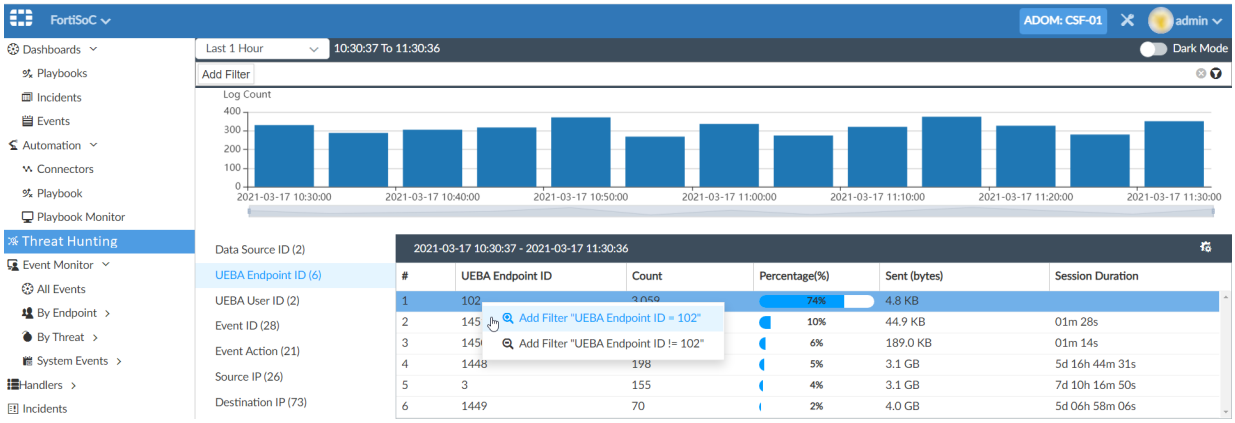
The dashboard includes a predefined time filter to specify the time range you want to view. You can manually drag the progress bar below the *Log Count* graph to display the chart in different time ranges, and the data will change accordingly.



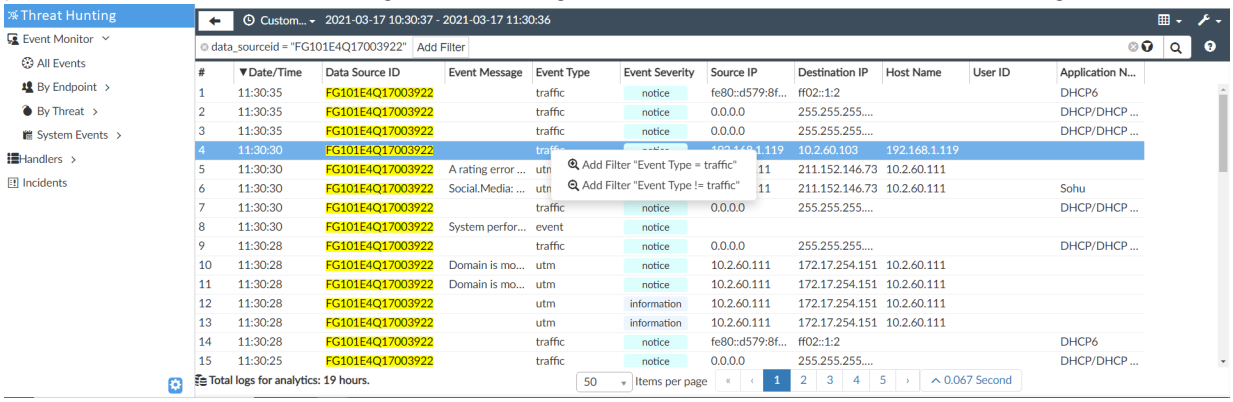
The left pane includes a list of selectable fields of interest. The right pane provides analytics to display the actual values for the selected field with statistics in the selected time range.



2. Right-click on a value in the table to add it to a filter. Fields in the left pane and Log Count chart are updated.



3. Double-click a column of interest on the right pane to drilldown and see detailed log information. The drilldown view provides the same functions as Log View, including a search bar filter, time filter, columns setting.

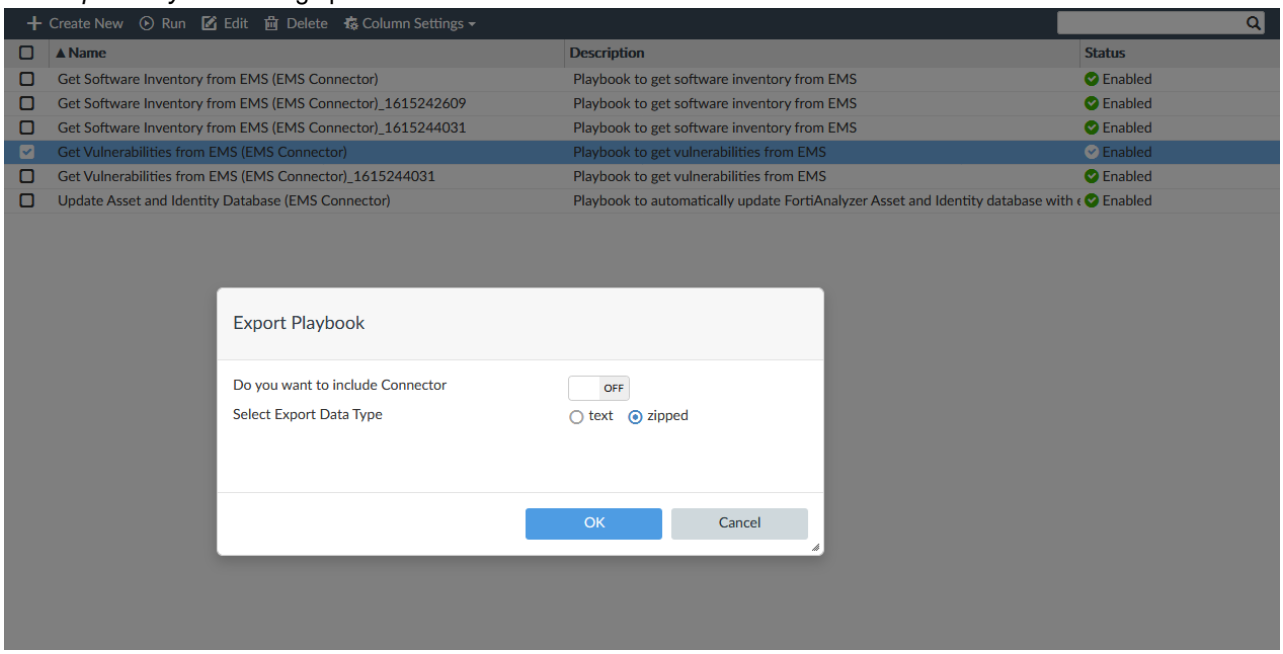


Importing and exporting playbooks

This feature adds the ability to import/export playbooks with the option to include connector data.

To export a playbook:

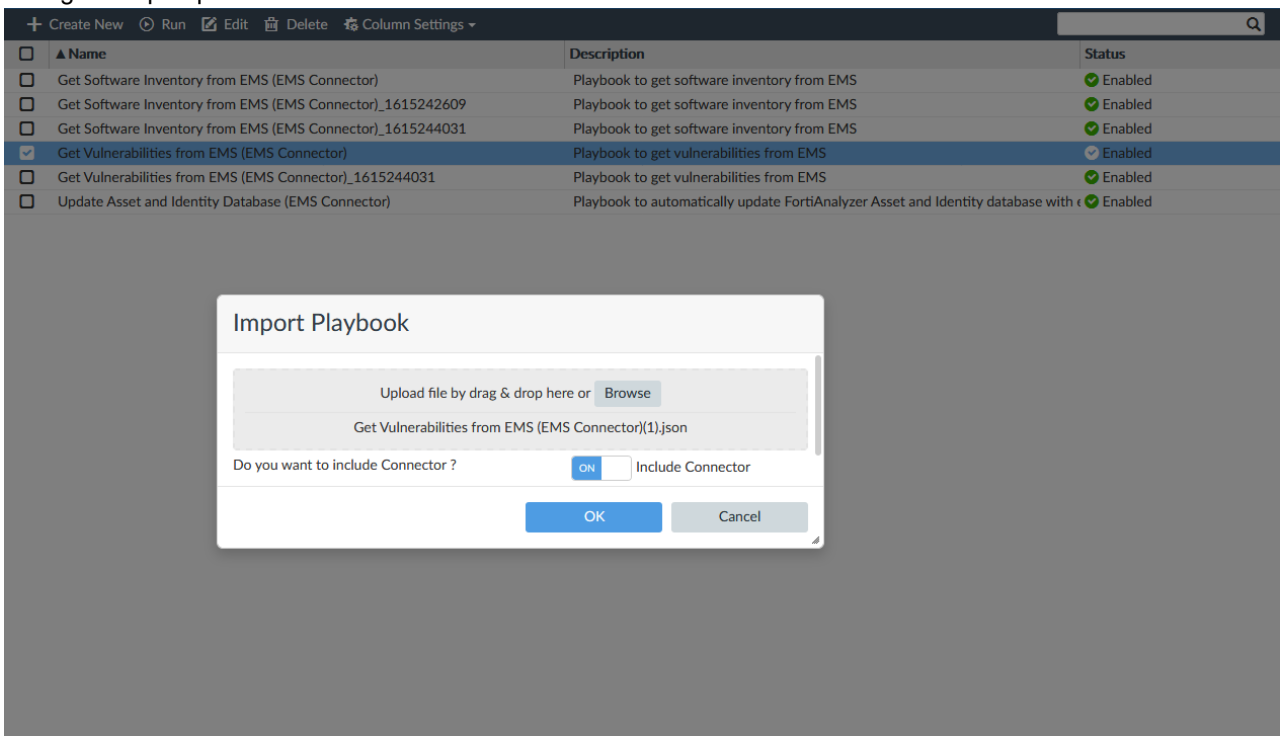
1. Go to *FortiSoC* > *Automation* > *Playbook*.
2. Highlight the playbook(s) that you want to export, then right-click in the dashboard and click *Export*. The *Export Playbook* dialog opens.



3. Configure the settings for exporting the selected playbook:
   a. *Do you want to include Connector*: When enabled, connector configurations required to run this playbook will be included in the exported file.
   b. *Select Export Data Type*: Select the export file type as either plain text JSON or zipped/base 64 encoded JSON.
4. Click *OK*. The file will be downloaded locally and is viewable within another editor when in the plain text format.

To import a playbook:

1. Go to *FortiSoC* > *Automation* > *Playbook* in another FortiAnalyzer ADOM.
2. Right-click in the playbook dashboard, and click *Import*.
   The *Import Playbook* dialog appears.
3. Click *Browse* and select the playbook file to be imported. .
   When the playbook file includes connectors, you will see a toggle allowing you to include or exclude the connectors during the import process.



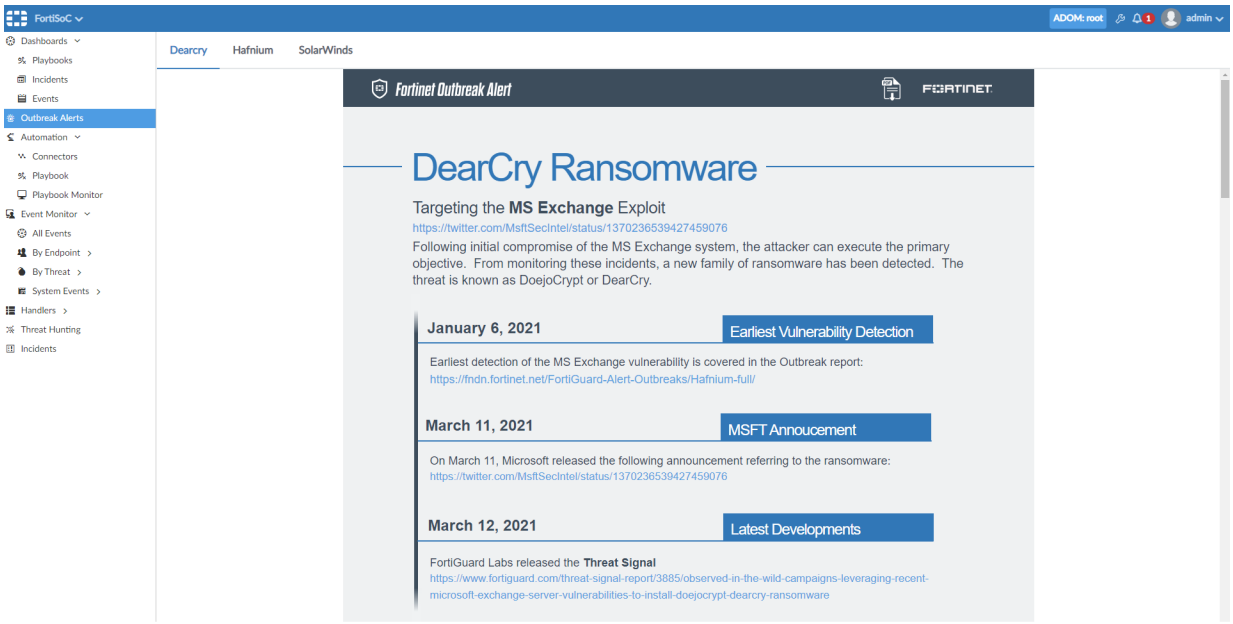
4. Click *OK*. A message is displayed to confirm that the playbook was imported successfully.
   When a playbook or connector being imported shares the same name as an existing one, a new name will be created which includes the timestamp. Playbooks will be automatically updated with the new connector name.

FortiGuard outbreak and alert service

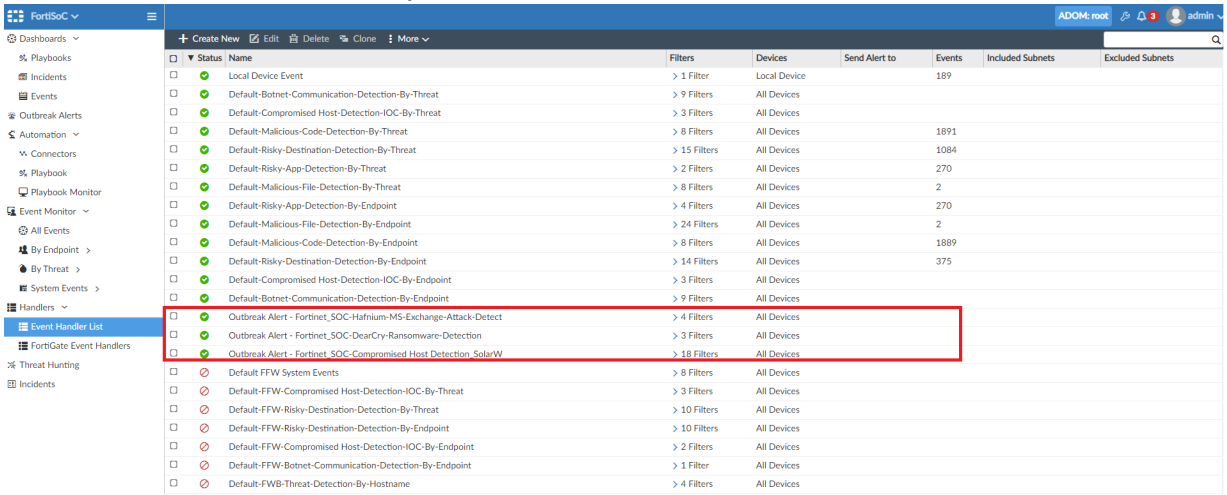
A new FortiGuard Outbreak Alert Service (FOAS) is now available through the Enterprise Protection bundle to protect customer's networks against malware outbreaks. The Outbreak Alert content package consists of a FortiGuard Report for the outbreak, an Event Handler, and a Report Template to detect the outbreak.

To view outbreak alerts, reports, and event handlers:

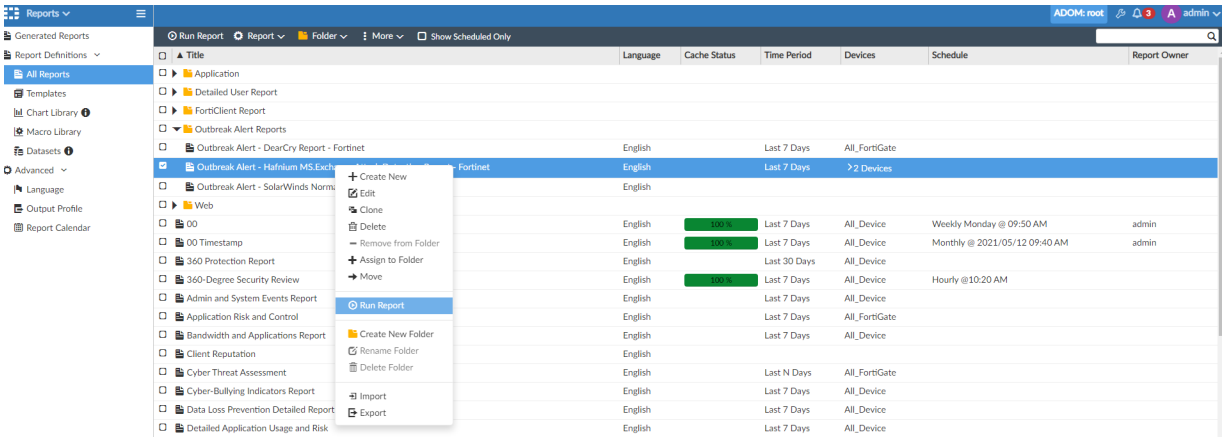
1. Go to *FortiSoC* > *Outbreak Alerts*. Available outbreak alerts, including DearCry, Hafnium, and SolarWinds, are displayed and can be browsed in all ADOMs.
   The outbreak alert can be downloaded by clicking on the download icon.



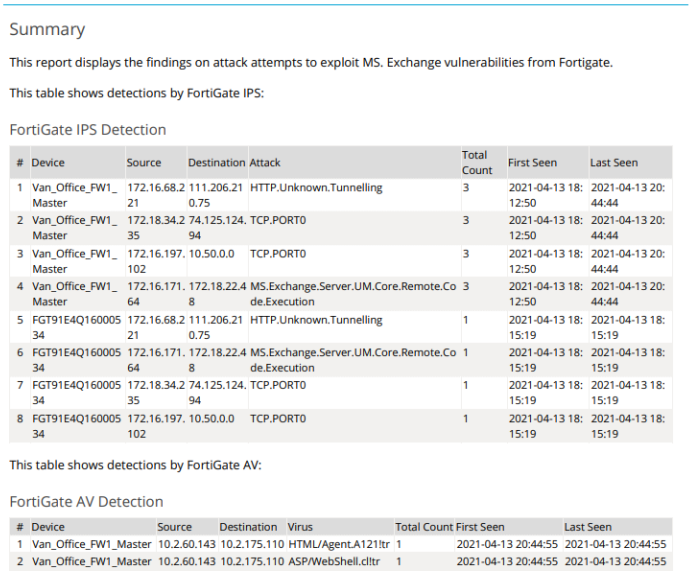
2. Go to *FortiSoC* > *Handlers* > *Event Handler List*. Corresponding outbreak alert event handlers are installed and listed in related ADOMs automatically.



3. Go to *Reports* > *Report Definitions* > *All Reports*.
A new *Outbreak Alert Reports* folder is available in all ADOMs. All outbreak reports are stored in this folder. Current outbreak reports include *DearCry Report*, *Hafnium M.S.Exchange Attack Detection Report*, and *SolarWinds Normalized Report*, available in Fabric ADOMs.
Right click a report to run the report. Reports can be generated in HTML, PDF, XML, and CSV formats.



Below is an example of the *Hafnium M.S.Exchange Attack Detection Report*.



Summary

This report displays the findings on attack attempts to exploit MS. Exchange vulnerabilities from Fortigate.

This table shows detections by FortiGate IPS:

FortiGate IPS Detection

#	Device	Source	Destination	Attack	Total Count	First Seen	Last Seen
1	Van_Office_FW1_Master	172.16.68.221	111.206.210.75	HTTP.Unknown.Tunnelling	3	2021-04-13 18:12:50	2021-04-13 20:44:44
2	Van_Office_FW1_Master	172.18.34.235	74.125.124.94	TCP.PORT0	3	2021-04-13 18:12:50	2021-04-13 20:44:44
3	Van_Office_FW1_Master	172.16.197.102	10.50.0.0	TCP.PORT0	3	2021-04-13 18:12:50	2021-04-13 20:44:44
4	Van_Office_FW1_Master	172.16.171.64	172.18.22.48	MS.Exchange.Server.UM.Core.Remote.Code.Execution	3	2021-04-13 18:12:50	2021-04-13 20:44:44
5	FGT91E4Q16000534	172.16.68.221	111.206.210.75	HTTP.Unknown.Tunnelling	1	2021-04-13 18:15:19	2021-04-13 18:15:19
6	FGT91E4Q16000534	172.16.171.64	172.18.22.48	MS.Exchange.Server.UM.Core.Remote.Code.Execution	1	2021-04-13 18:15:19	2021-04-13 18:15:19
7	FGT91E4Q16000534	172.18.34.235	74.125.124.94	TCP.PORT0	1	2021-04-13 18:15:19	2021-04-13 18:15:19
8	FGT91E4Q16000534	172.16.197.102	10.50.0.0	TCP.PORT0	1	2021-04-13 18:15:19	2021-04-13 18:15:19

This table shows detections by FortiGate AV:

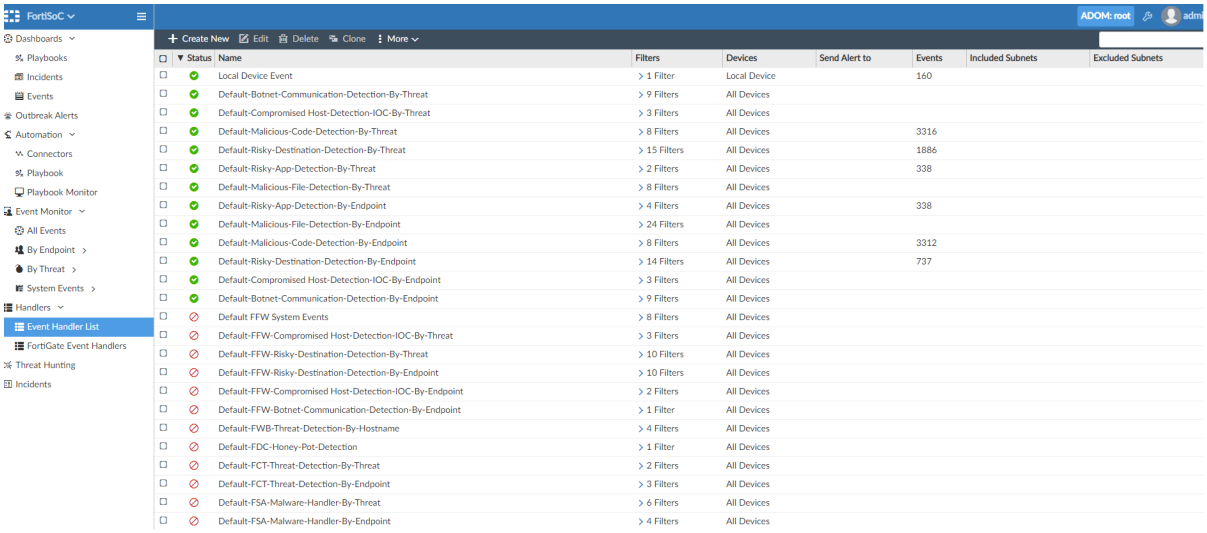
FortiGate AV Detection

#	Device	Source	Destination	Virus	Total Count	First Seen	Last Seen
1	Van_Office_FW1_Master	10.2.60.143	10.2.175.110	HTML/Agent.A121!tr	1	2021-04-13 20:44:55	2021-04-13 20:44:55
2	Van_Office_FW1_Master	10.2.60.143	10.2.175.110	ASP/WebShell.cl!tr	1	2021-04-13 20:44:55	2021-04-13 20:44:55

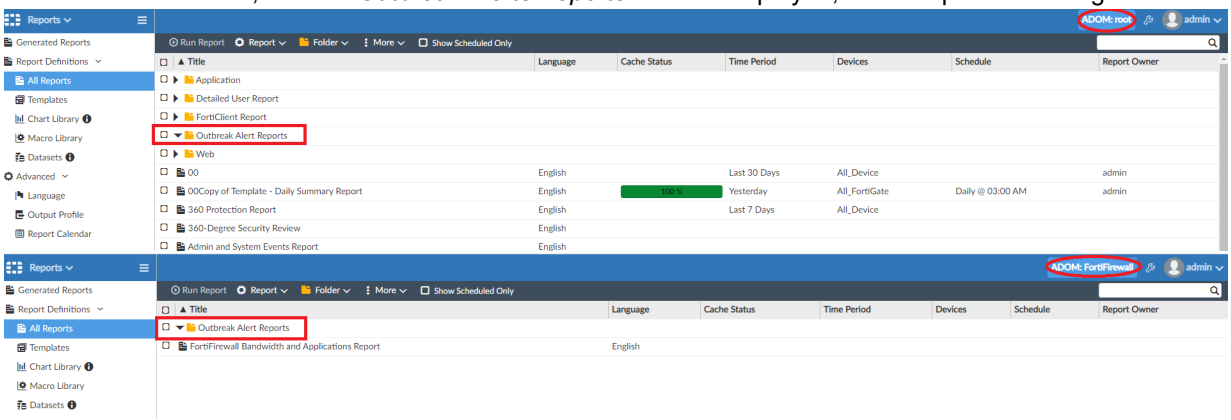
4. When FortiAnalyzer does not have a valid FOAS license, a default Fortinet Outbreak Alert page is displayed with a reminder that to get outbreak alert services, you need a license. The option to download outbreak alerts is not

available until you have a valid license.

5. Go to *FortiSoC* > *Handlers* > *Event Handler List*.
Without a valid license, no outbreak related event handlers are available.



6. Go to *Reports* > *Report Definitions* > *All Reports*.
   Without a valid license, the new *Outbreak Alerts Reports* folder is displayed, but no reports are assigned to it.



To configure FortiGuard settings in the CLI:

1. In the FortiAnalyzer CLI, enter the following command:

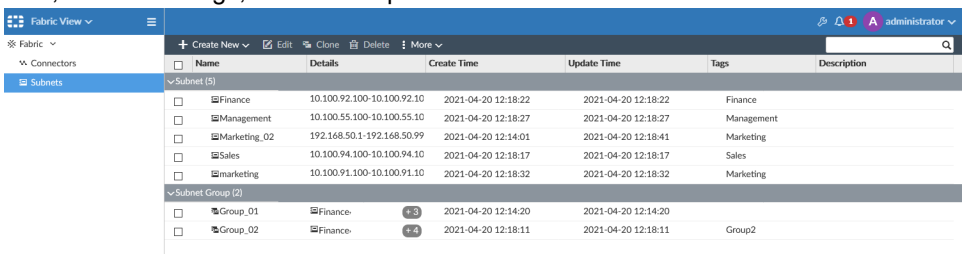
```
config fmupdate fds-setting
(fds-setting) # show
config fmupdate fds-setting
config server-override
set status enable
config servlist
edit 1
set ip 192.168.X.X
```

Manage subnets

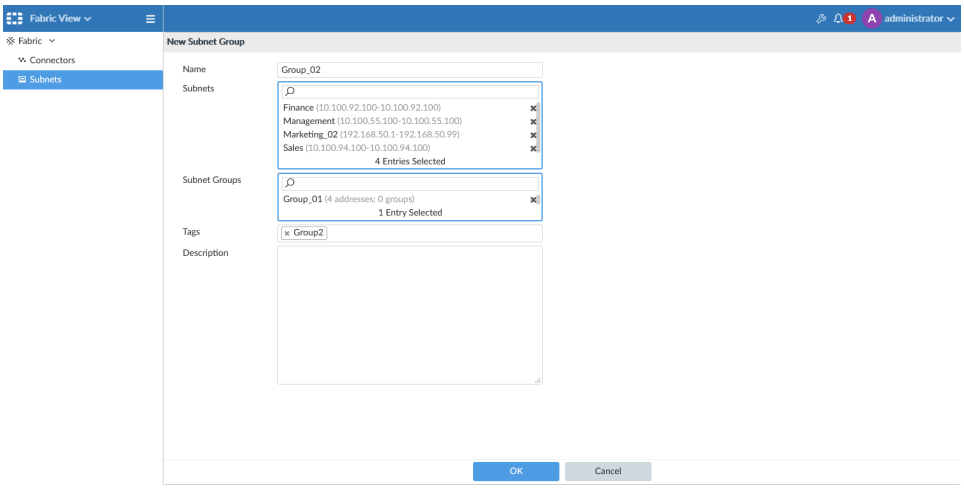
Enhanced subnets configuration and management is now available from *Fabric View* with additional support for nested subnet groups and tags.

To view enhanced subnets in FortiAnalyzer:

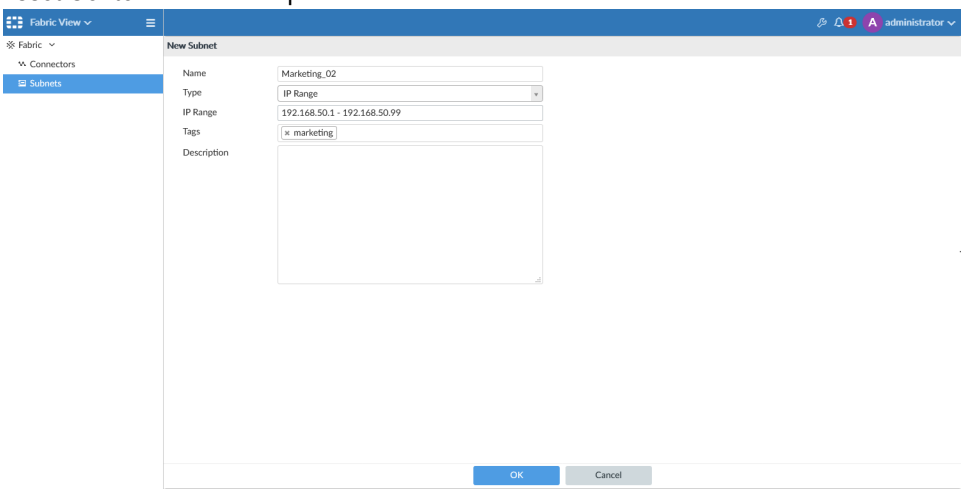
1. Go to *Fabric View* > *Fabric* > *Subnets*.
   The subnets and subnet groups table is shown displaying additional information including the created time, update time, associated tags, and a description.



2. Edit or create a new subnet group.
   Subnet groups have additional configurable options including a description field and tag support. Tags are shown in the *Asset Center* list if the endpoint IP falls within the subnet group.
   Subnet groups support nested groups as members.



3. Edit or create a new subnet.
   Subnets have additional configurable options including a description field and tag support. Tags are shown in the *Asset Center* list if the endpoint IP falls within the subnet.



4. Go to *Log View* > *FortiAnalyzer* > *Events*. Local events are generated when subnets are created, updated, or deleted.
5. Reports and Event Handlers can use subnets as filters.

Incident and Event Management

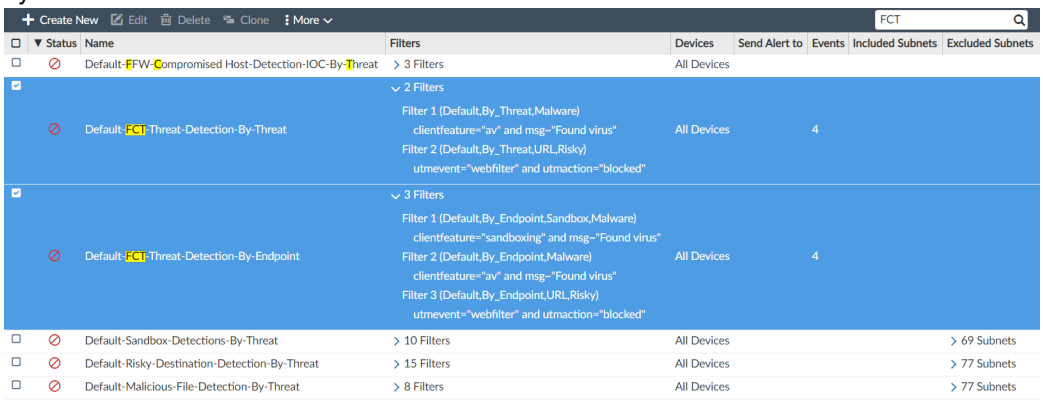
This section lists the new features added to FortiAnalyzer for incident and event management:

FortiClient event handler update

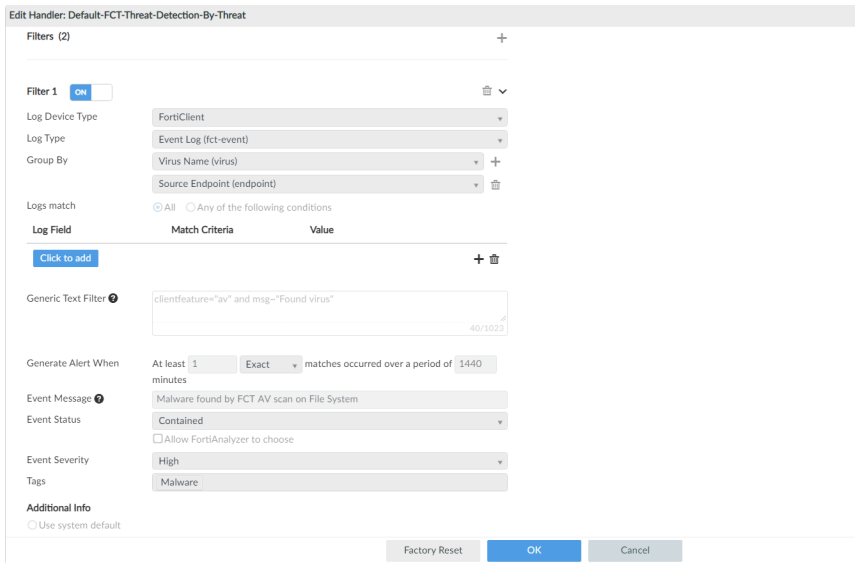
The predefined FortiClient event handlers are updated to include the detection from the newly added logs.

To view the updated FortiClient event handlers:

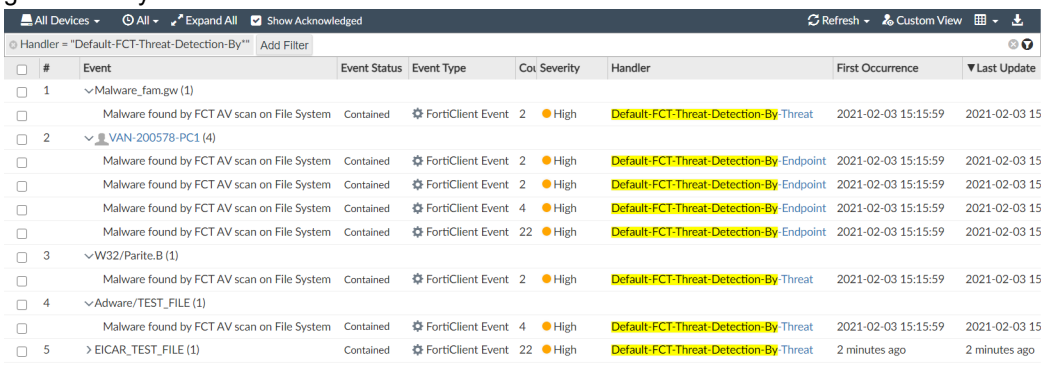
1. Go to *FortiSoC* > *Handlers* > *Event Handler List*.
   Predefined handlers providing threat detection on FortiClient logs are available. These event handlers are disabled by default.



2. Double-click a FortiClient event handler to view filter details.



3. In the event handler list, right-click a FortiClient event handler and select *Enable*. After being enabled, events will be generated by the event handler.

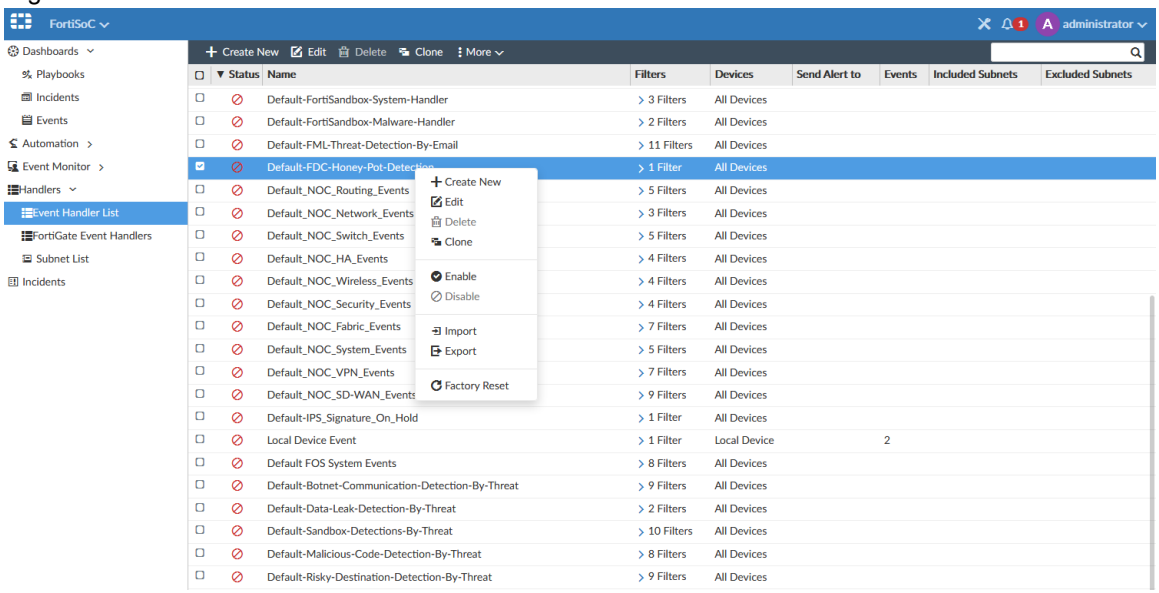


FortiDeceptor default handler

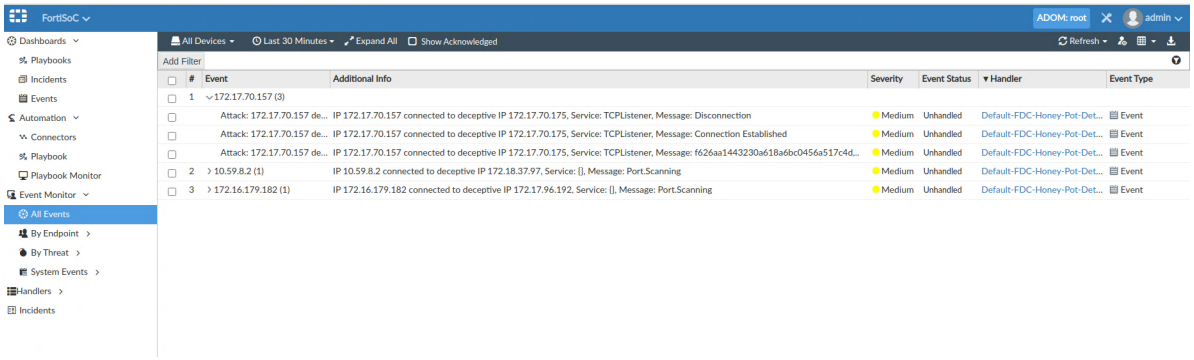
This is a new default handler that helps detect early breach activities and identify threats.

To use the FortiDeceptor default handler:

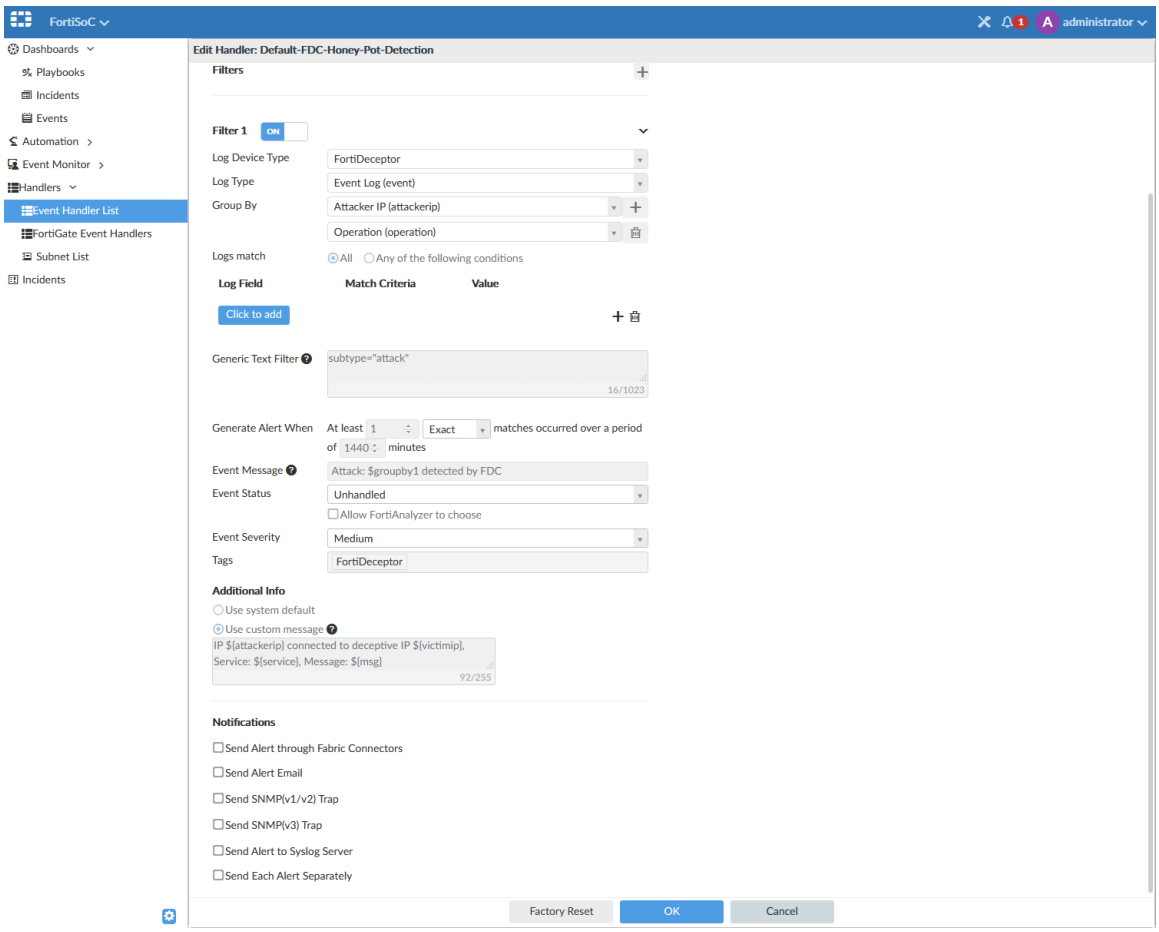
1. Go to *FortiSoC* > *Handlers* > *Event Handler List*.
   In the event handler list, find *Default-FDC-Honey-Pot-Detection*.
2. Right-click on the handler and select *Enable*.



The handler is now enabled. Below is an example of some events generated by the handler.



3. Double click on the handler in the list to review its filter details.

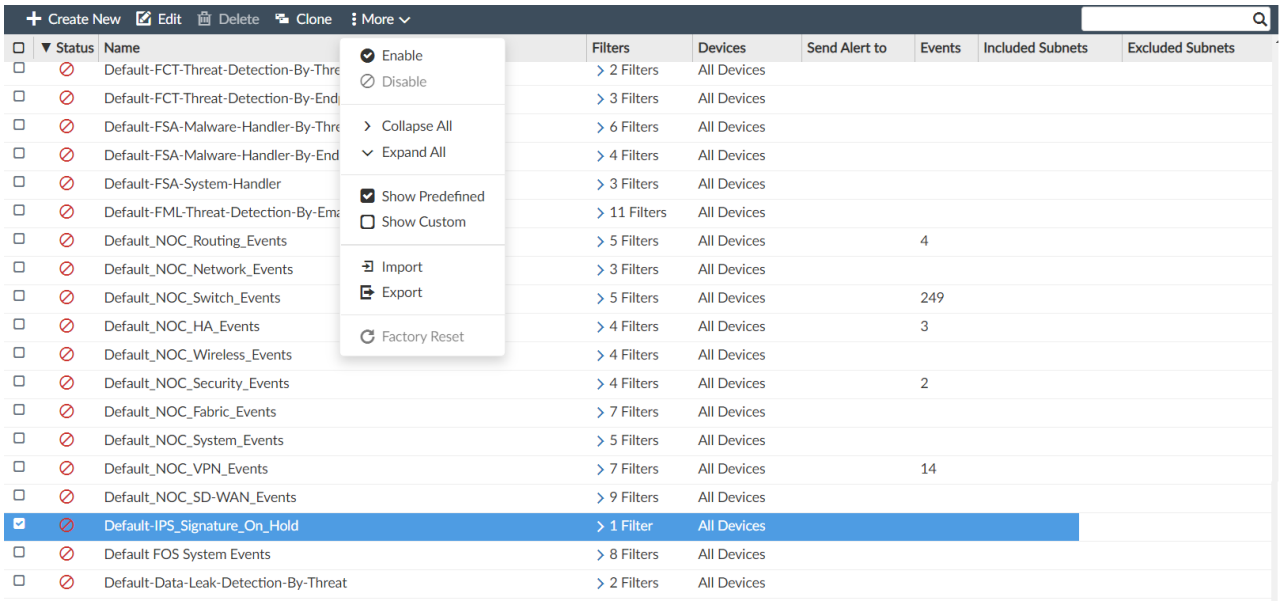


IPS signatures on-hold event handler

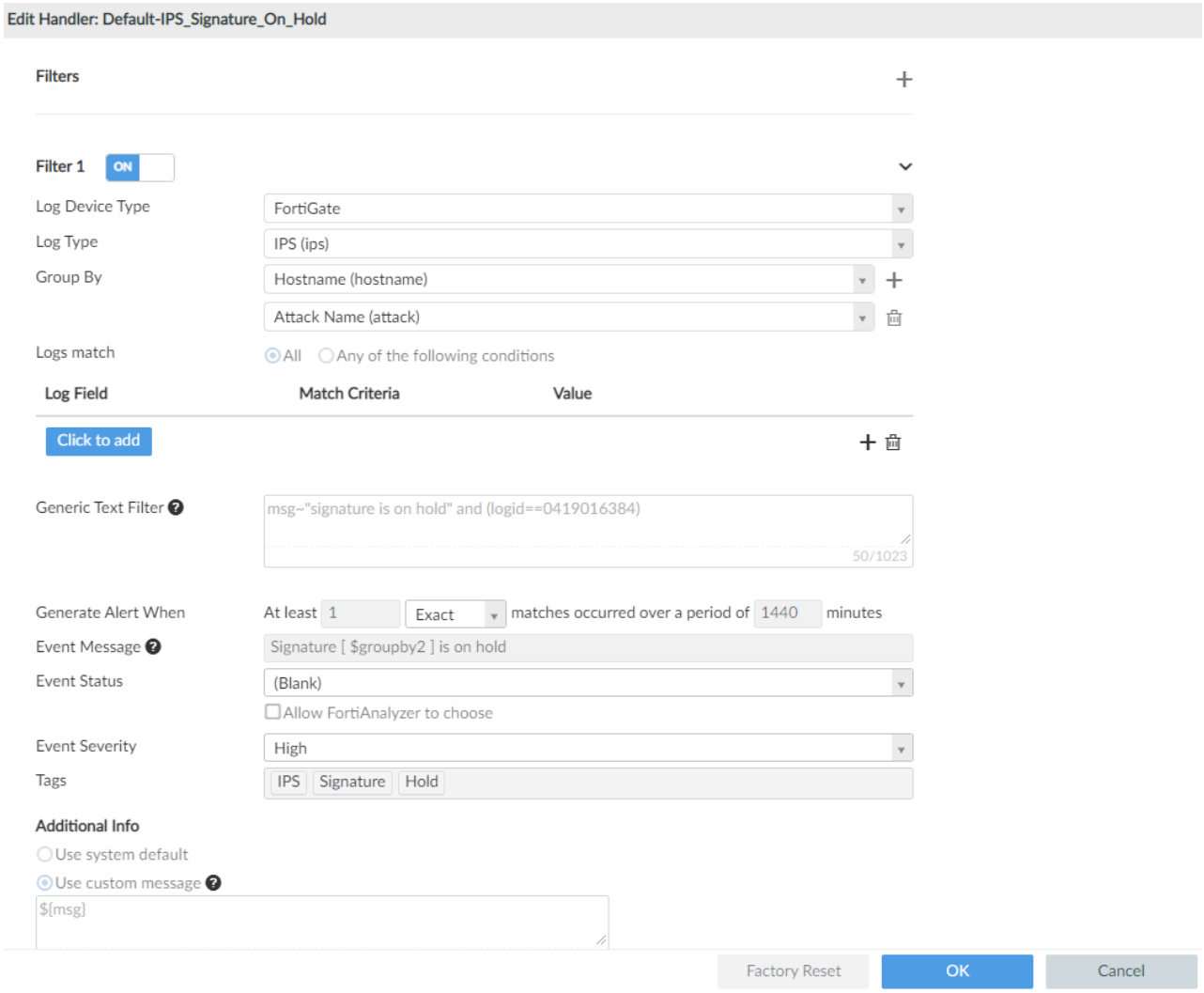
A new event handler is available for admins to monitor FortiGate IPS logs for the IPS signatures that are on hold.

To use the IPS signatures on-hold event handler:

1. Go to *FortiSoC > Handlers > Event Handler List*.
   The *Default-IPS_Signature_On_Hold* event handler is displayed and is disabled by default.



Double-click the event handler to view its filter definition.



2. Right-click on the event handler in the event handlers list, and click *Enable*. Events will be generated for IPS signature that are on hold.

NOC event handlers

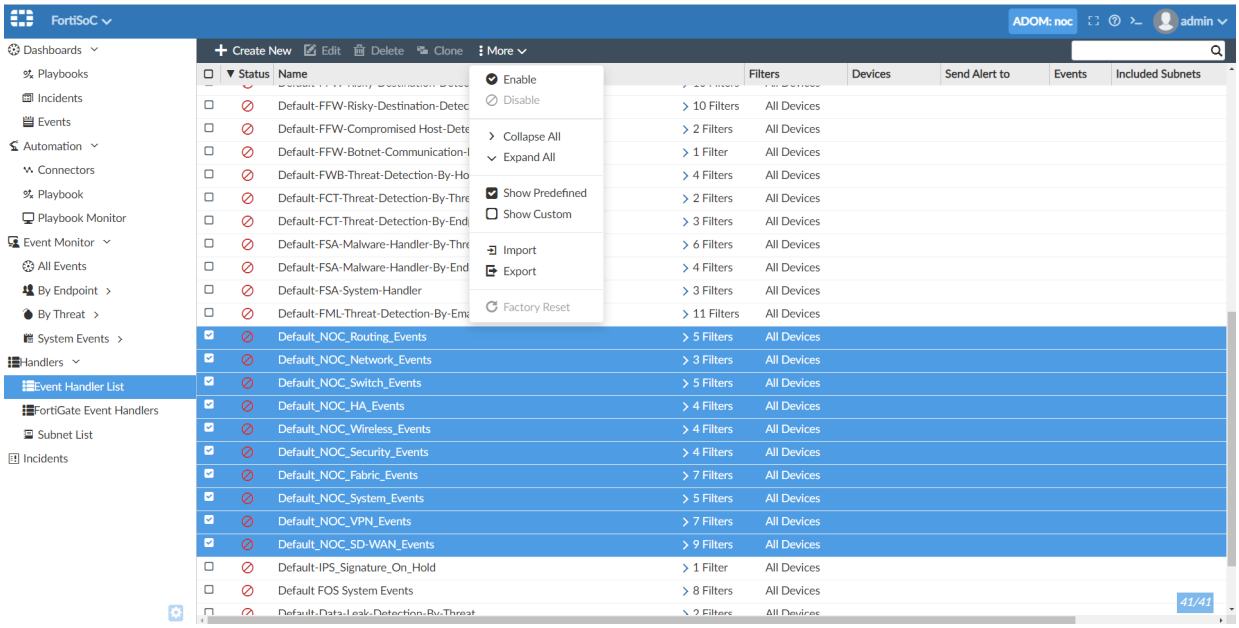
A new set of default event handlers are available for NOC to monitor network events and detect problems for routing, switching, wireless and more.

The following NOC event handlers are available in the *Event Handler List*:

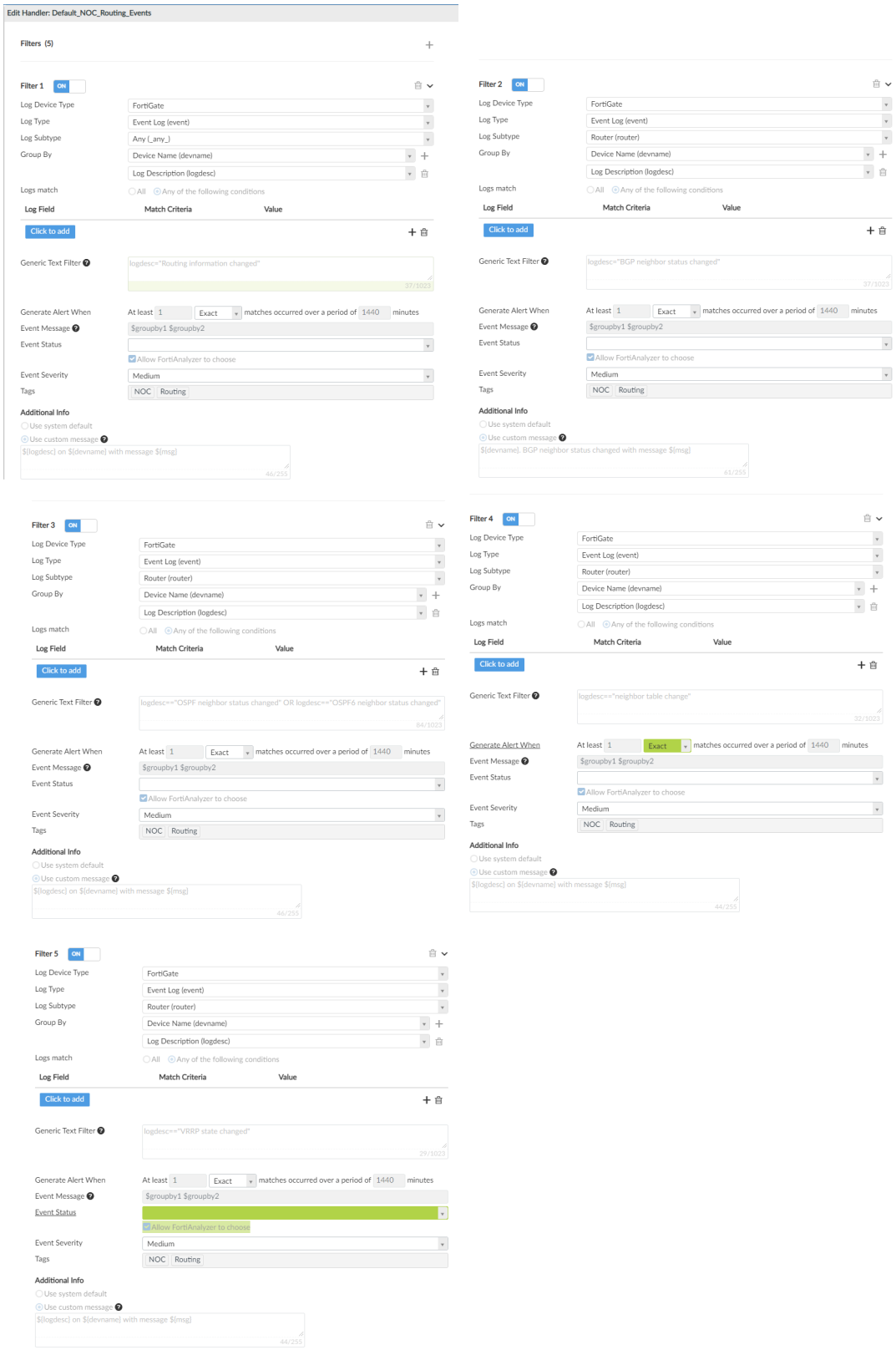
- `Default_NOC_Routing_Events`
- `Default_NOC_Network_Events`
- `Default_NOC_Switch_Events`
- `Default_NOC_HA_Events`
- `Default_NOC_Wireless_Events`
- `Default_NOC_Security_Events`
- `Default_NOC_Fabric_Events`
- `Default_NOC_System_Events`
- `Default_NOC_VPN_Events`
- `Default_NOC_SD-WAN_Events`

To enable NOC event handlers:

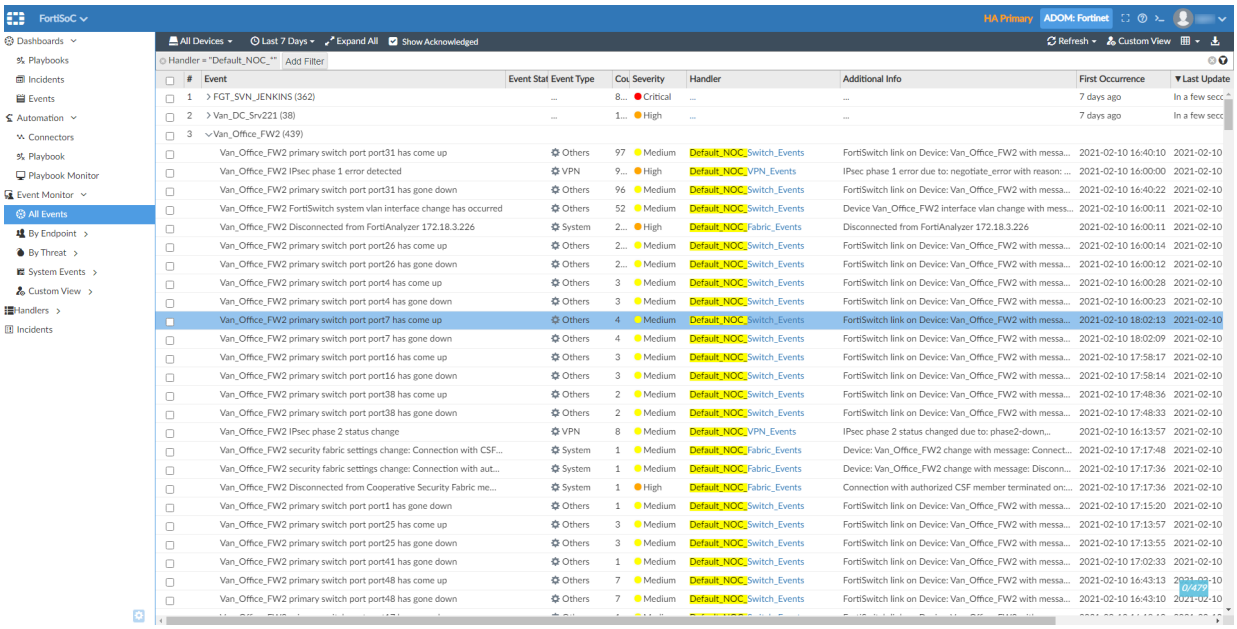
1. Go to *FortiSOC* > *Handlers* > *Event Handler List*.



2. Double-click a NOC event handler to view the predefined filters, and to enable notifications.



3. In the toolbar click *More* > *Enable*. The handler will generate events from a NOC perspective.



Dashboards

This section lists the new features added to FortiAnalyzer for dashboards:

- Shadow IT Monitoring Service on page 39
- Data sources tuning on page 42
- Asset and Identity Dashboards on page 46

Shadow IT Monitoring Service

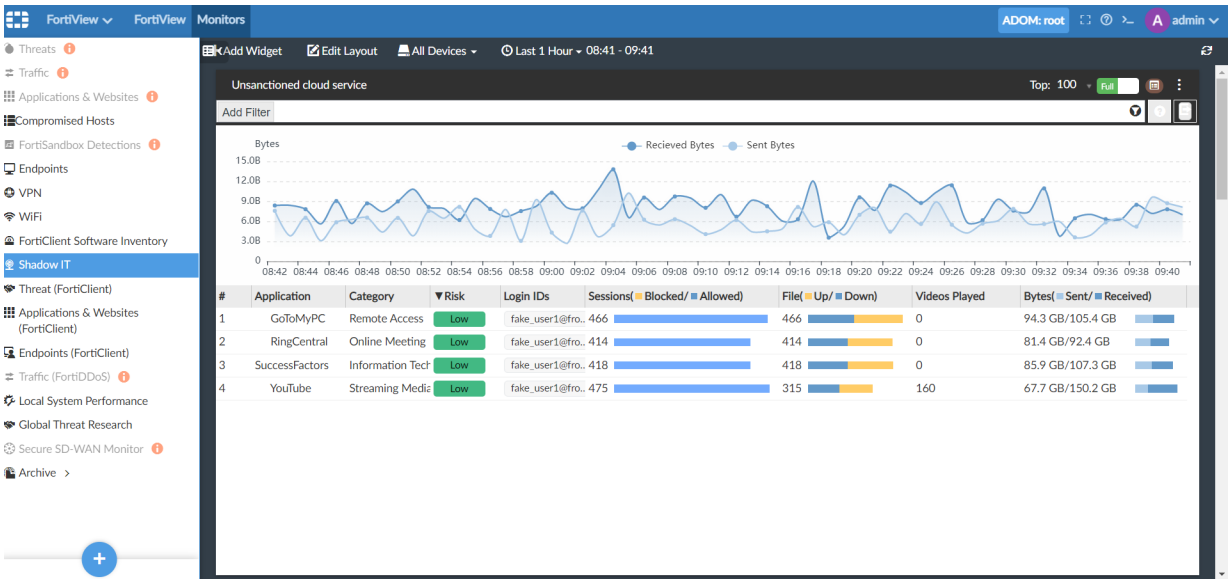
The Shadow IT dashboard continuously monitors customer environments by correlating data from FortiOS and FortiCASB to discover and investigate the risk of shadow IT and remediate and control the security risks.

To use this feature, you must have a FortiCASB account subscribed for SaaS features, and a FortiCASB connector configured on FortiAnalyzer.

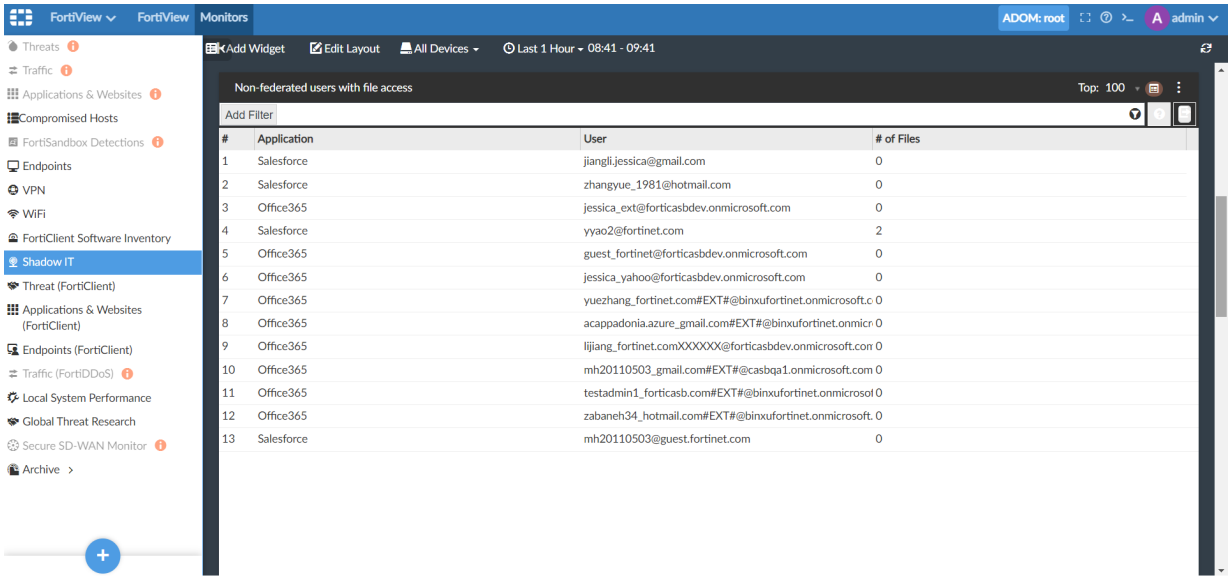
To view the Shadow IT dashboard:

1. Go to *FortiView* > *Monitors* and select *Shadow IT* from the tree menu.
   The Shadow IT dashboard has the following widgets:

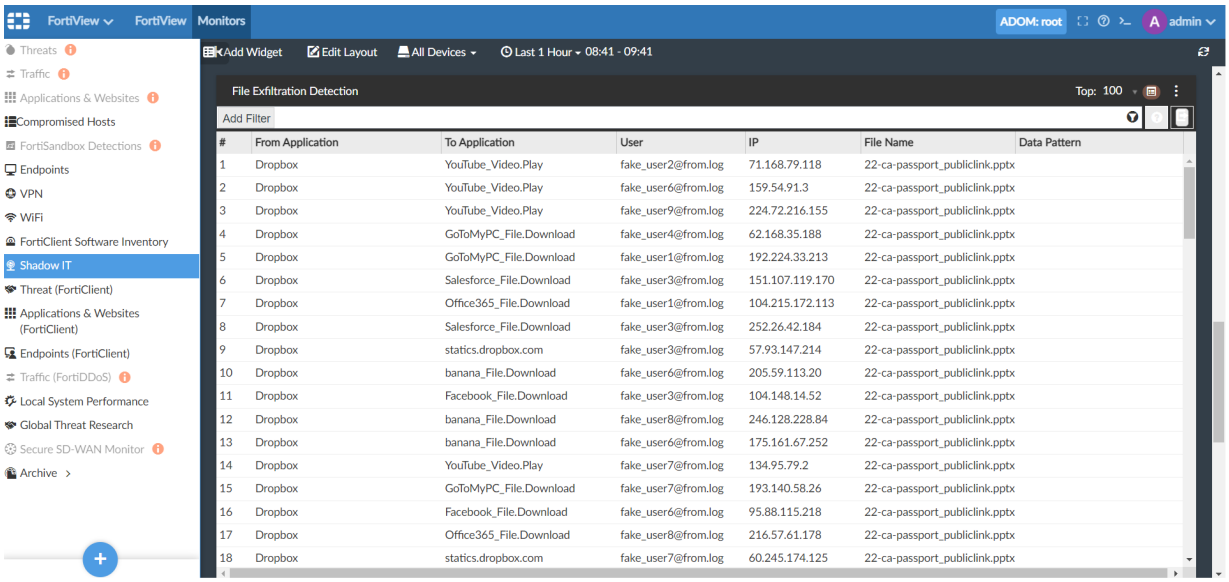
a. Unsanctioned Cloud Service.



b. Non-federated Users with File Access.

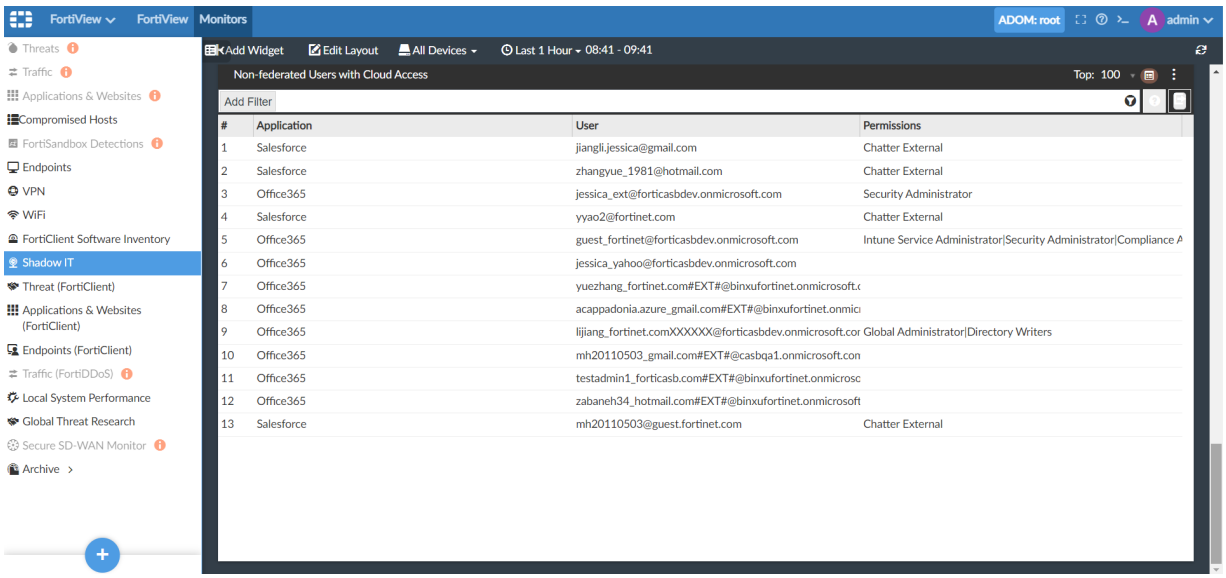


c. File Exfiltration Detection.



#	From Application	To Application	User	IP	File Name	Data Pattern
1	Dropbox	YouTube_Video.Play	fake_user2@from.log	71.168.79.118	22-ca-passport_publiclink.pptx	
2	Dropbox	YouTube_Video.Play	fake_user6@from.log	159.54.91.3	22-ca-passport_publiclink.pptx	
3	Dropbox	YouTube_Video.Play	fake_user9@from.log	224.72.216.155	22-ca-passport_publiclink.pptx	
4	Dropbox	GoToMyPC_File.Download	fake_user4@from.log	62.168.35.188	22-ca-passport_publiclink.pptx	
5	Dropbox	GoToMyPC_File.Download	fake_user1@from.log	192.224.33.213	22-ca-passport_publiclink.pptx	
6	Dropbox	Salesforce_File.Download	fake_user3@from.log	151.107.119.170	22-ca-passport_publiclink.pptx	
7	Dropbox	Office365_File.Download	fake_user1@from.log	104.215.172.113	22-ca-passport_publiclink.pptx	
8	Dropbox	Salesforce_File.Download	fake_user3@from.log	252.26.42.184	22-ca-passport_publiclink.pptx	
9	Dropbox	statics.dropbox.com	fake_user3@from.log	57.93.147.214	22-ca-passport_publiclink.pptx	
10	Dropbox	banana_File.Download	fake_user6@from.log	205.59.113.20	22-ca-passport_publiclink.pptx	
11	Dropbox	Facebook_File.Download	fake_user3@from.log	104.148.14.52	22-ca-passport_publiclink.pptx	
12	Dropbox	banana_File.Download	fake_user8@from.log	246.128.228.84	22-ca-passport_publiclink.pptx	
13	Dropbox	banana_File.Download	fake_user6@from.log	175.161.67.252	22-ca-passport_publiclink.pptx	
14	Dropbox	YouTube_Video.Play	fake_user7@from.log	134.95.79.2	22-ca-passport_publiclink.pptx	
15	Dropbox	GoToMyPC_File.Download	fake_user7@from.log	193.140.58.26	22-ca-passport_publiclink.pptx	
16	Dropbox	Facebook_File.Download	fake_user6@from.log	95.88.115.218	22-ca-passport_publiclink.pptx	
17	Dropbox	Office365_File.Download	fake_user8@from.log	216.57.61.178	22-ca-passport_publiclink.pptx	
18	Dropbox	statics.dropbox.com	fake_user7@from.log	60.245.174.125	22-ca-passport_publiclink.pptx	

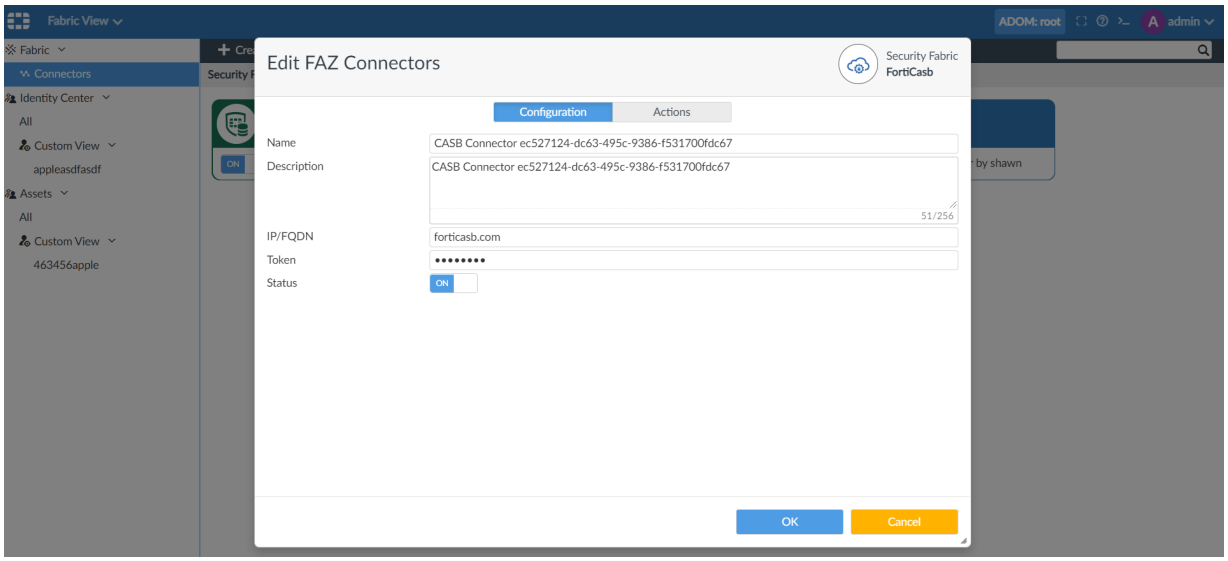
d. Non-federated Users with Cloud Access.



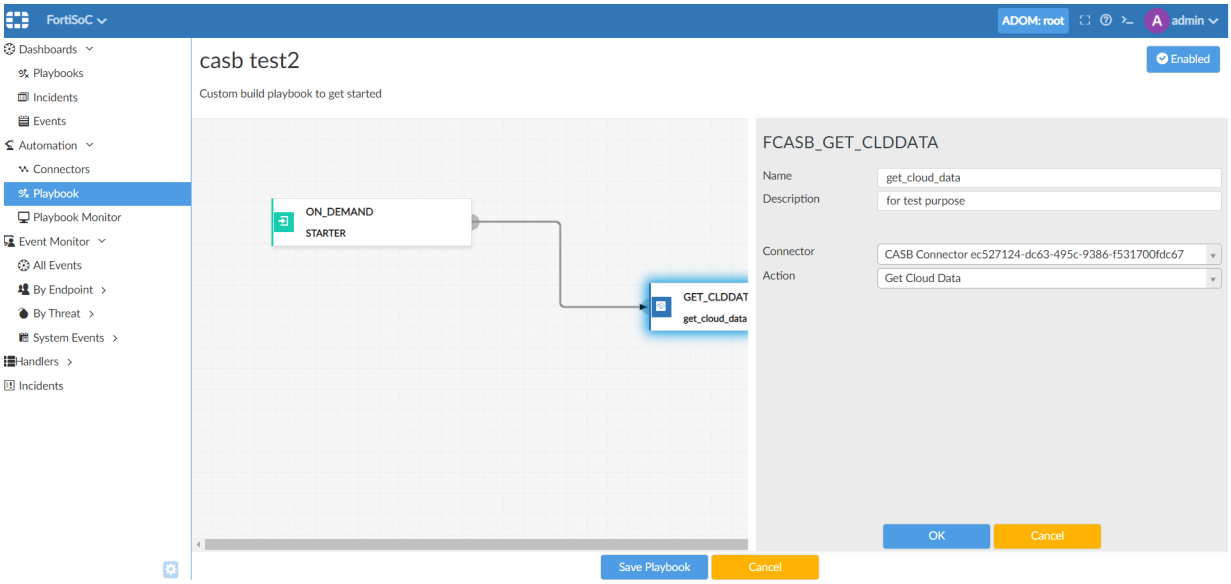
#	Application	User	Permissions
1	Salesforce	jiangli.jessica@gmail.com	Chatter External
2	Salesforce	zhangyue_1981@hotmail.com	Chatter External
3	Office365	jessica_ext@forticasbdev.onmicrosoft.com	Security Administrator
4	Salesforce	yyao2@fortinet.com	Chatter External
5	Office365	guest_fortinet@forticasbdev.onmicrosoft.com	Intune Service Administrator|Security Administrator|Compliance A
6	Office365	jessica_yahoo@forticasbdev.onmicrosoft.com	
7	Office365	yuezhang_fortinet.com#EXT#@binxufortinet.onmicrosoft.c	
8	Office365	acappadonia.azure_gmail.com#EXT#@binxufortinet.onmici	
9	Office365	lijiang_fortinet.comXXXXXX@forticasbdev.onmicrosoft.cor	Global Administrator|Directory Writers
10	Office365	mh20110503_gmail.com#EXT#@casbqa1.onmicrosoft.con	
11	Office365	testadmin1_forticasb.com#EXT#@binxufortinet.onmicrosc	
12	Office365	zabaneh34_hotmail.com#EXT#@binxufortinet.onmicrosoft	
13	Salesforce	mh20110503@guest.fortinet.com	Chatter External

2. In order for FortiAnalyzer to correlate data from FortiGate and FortiCASB to generate the log data used in the Shadow IT monitor, an administrator must configure the FortiCASB connector in FortiAnalyzer's *Fabric View*. When creating or editing a FortiCASB connector, enter the following information:
   - **Name**: Enter a name for the FortiCASB connector.
   - **Description**: (Optional) Enter a description of the connector.
   - **IP/FQDN**: Enter the FortiCASB FQDN for your chosen server location. The server location is selected when creating your FortiCASB account. Use `forticasb.com` for global servers or `eu.forticasb.com` for EU based servers.
   - **Token**: Enter the credentials token used for authentication. To create a FortiCASB credentials token, log in to FortiCASB with your account, go to *Home* > *Manage Company* > *API Setting*, and click *Generate New*. For more information, see *FortiCASB* on the Fortinet Docs Library.

- **Status**: Set the status to *ON*.



3. To retrieve cloud application, users, and sensitive file information from FortiCASB on demand, an administrator can configure a playbook on FortiAnalyzer in FortiSOC. The playbook must include a task configured with the FortiCASB connector and *Get Cloud Data* action.

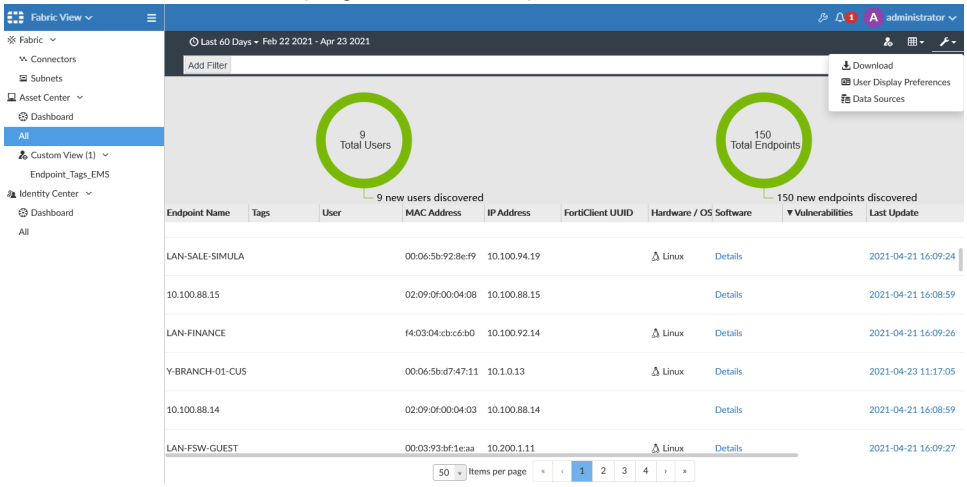


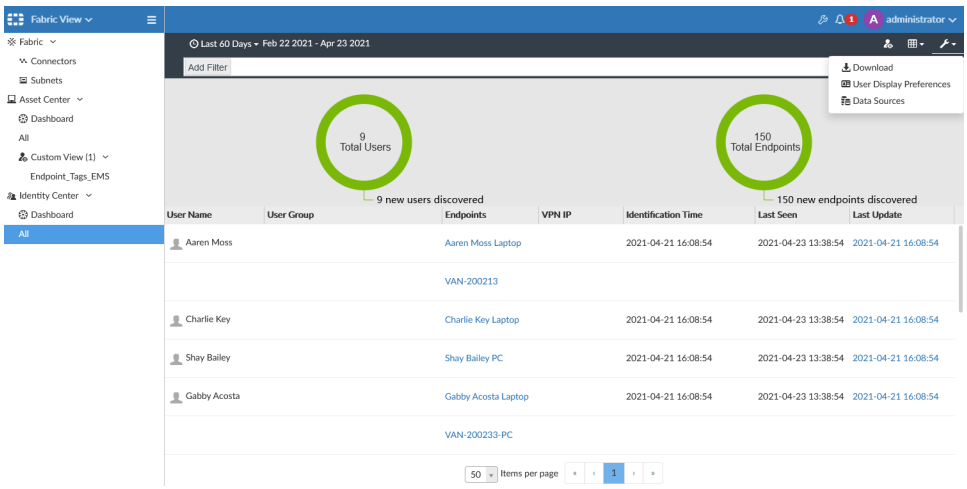
Data sources tuning

FortiAnalyzer 7.0.0 includes the option to have more granular control on data sources from the Asset Center and Identity Center - subnets can now be excluded from the selected data sources to reduce noise.

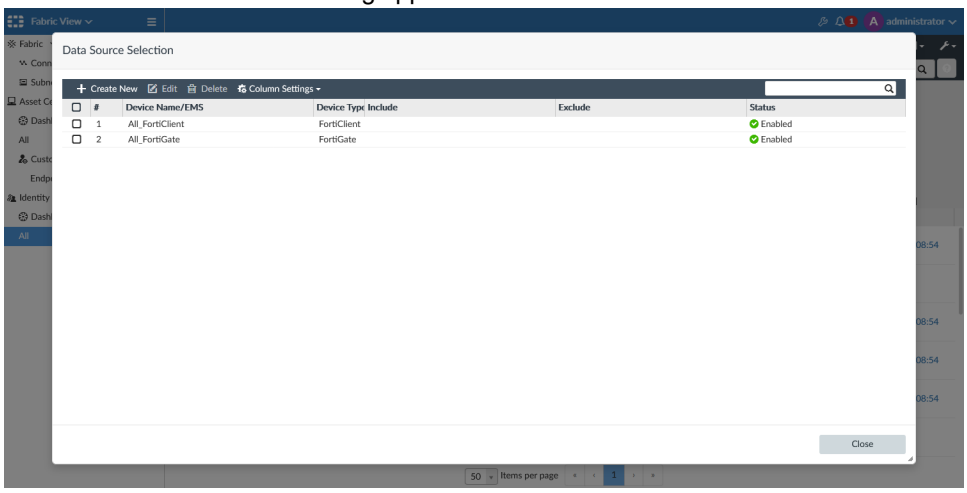
To configure data sources:

1. Go to *Fabric View* > *Identity Center* > *All* or *Fabric View* > *Asset Center* > *All*.
2. Click the tools icon in the top-right corner of the pane, and select *Data Sources*.



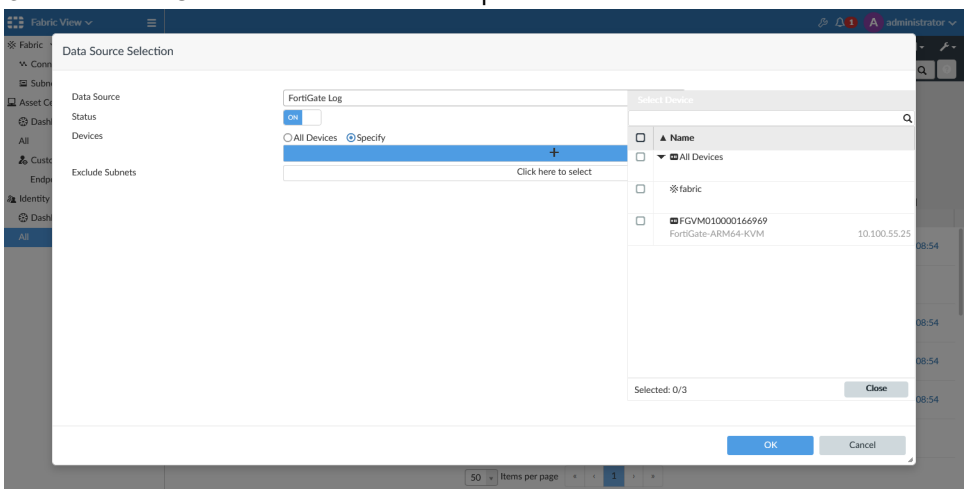


The *Data Source Selection* dialog appears.

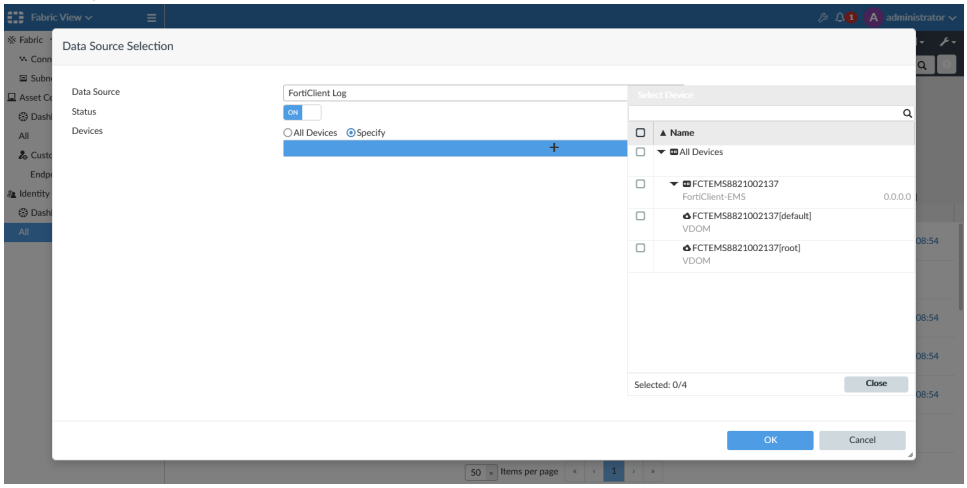


3. Click *Create New* to configure a new data source. Six data source types are available:
   - **FortiGate Log**:
     By default, the log identification of endpoints and end users is enabled for all devices and subnets. You can

create rules to specify which devices and which subnets can be excluded in the data source. Set the status to *OFF* to disable UEBA identification on the specified devices or all devices.

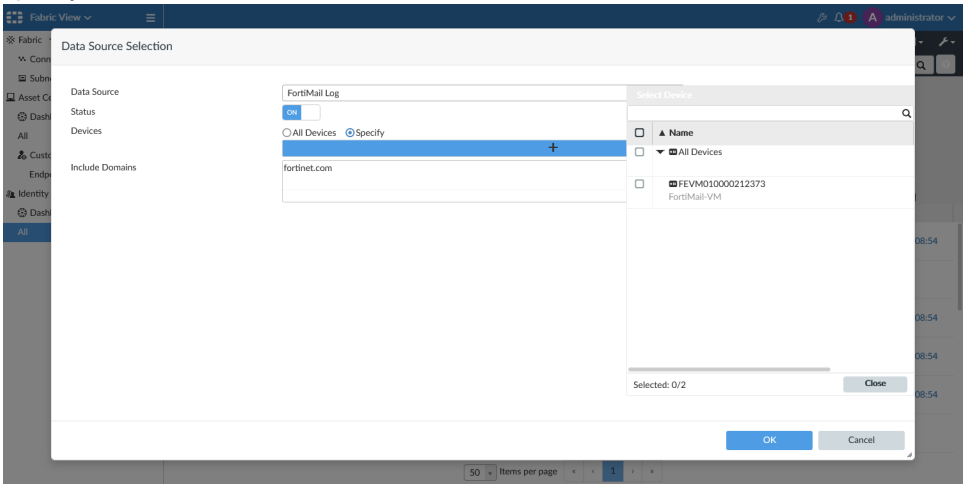


- **FortiClient Log**:
  By default, the log identification of endpoints and end users is enabled for all devices. You can create rules to specify which devices can be excluded in the data source. Set the status to *OFF* to disable UEBA identification on the specified devices or all devices.

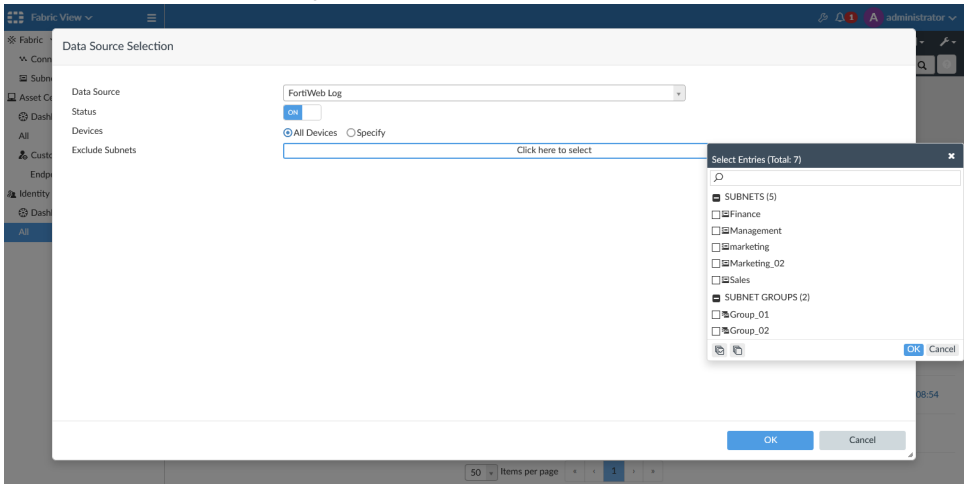


- **FortiMail Log**:
  By default, the log identification of endpoints and end users is disabled for all devices. You can create rules to

specify which devices and domains can be included in the data source.

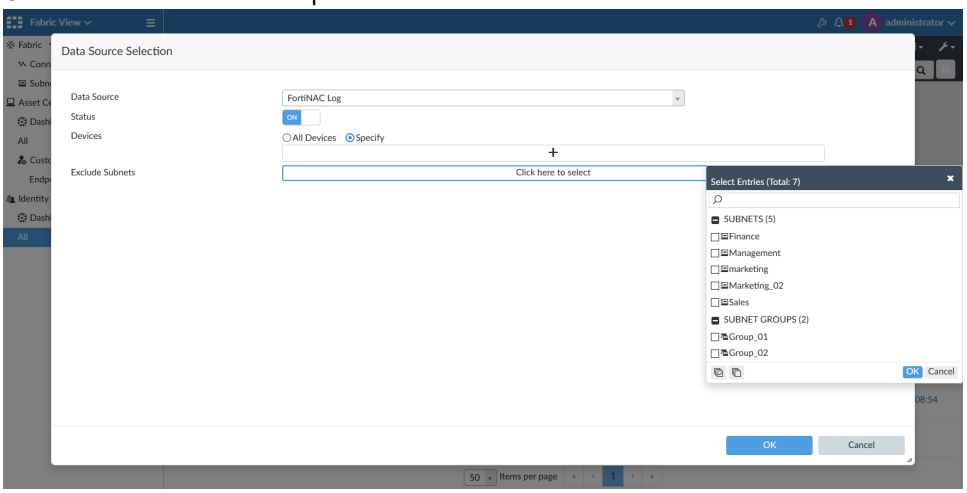


- **FortiWeb Log**:
  By default, the log identification of endpoints and end users is enabled for all devices. You can create rules to specify which devices and which subnets can be excluded in the data source. Set the status to *OFF* to disable UEBA identification on the specified devices or all devices.

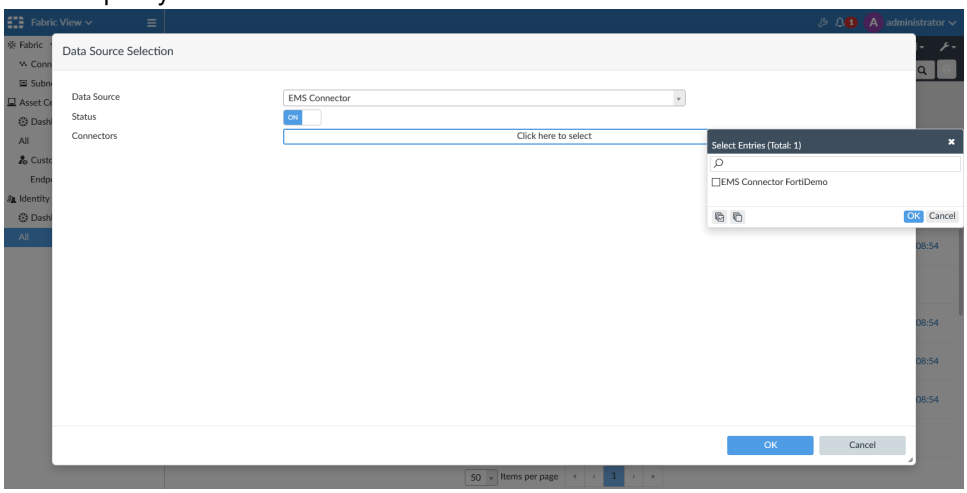


- **FortiNAC Log**:
  By default, the log identification of endpoints and end users is enabled for all devices. You can create rules to specify which devices and which subnets can be excluded in the data source. Set the status to *OFF* to disable

UEBA identification on the specified devices or all devices.



- **EMS Connector**:
  By default, the log identification of endpoints and end users is disabled for all EMS connectors. You can create rules to specify which connectors can be included in the data source.



Rules on individual devices have higher priority than the rules configured for "All Devices". You can configure the same data source multiple times when the device or connector is unique. When a conflict arises, you will see a message indicating the data source for that device already exists, and you will have the option to override the existing data source.

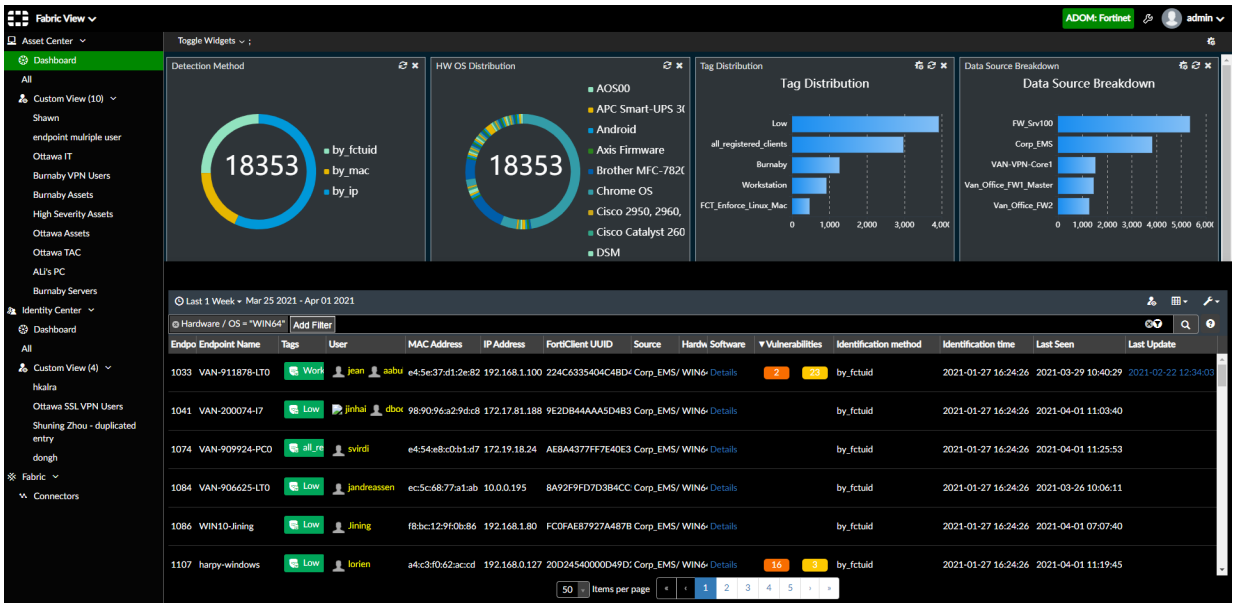
Asset and Identity Dashboards

Dedicated Assets/Identity dashboards to provide the SOC team better visibility on assets and their users.

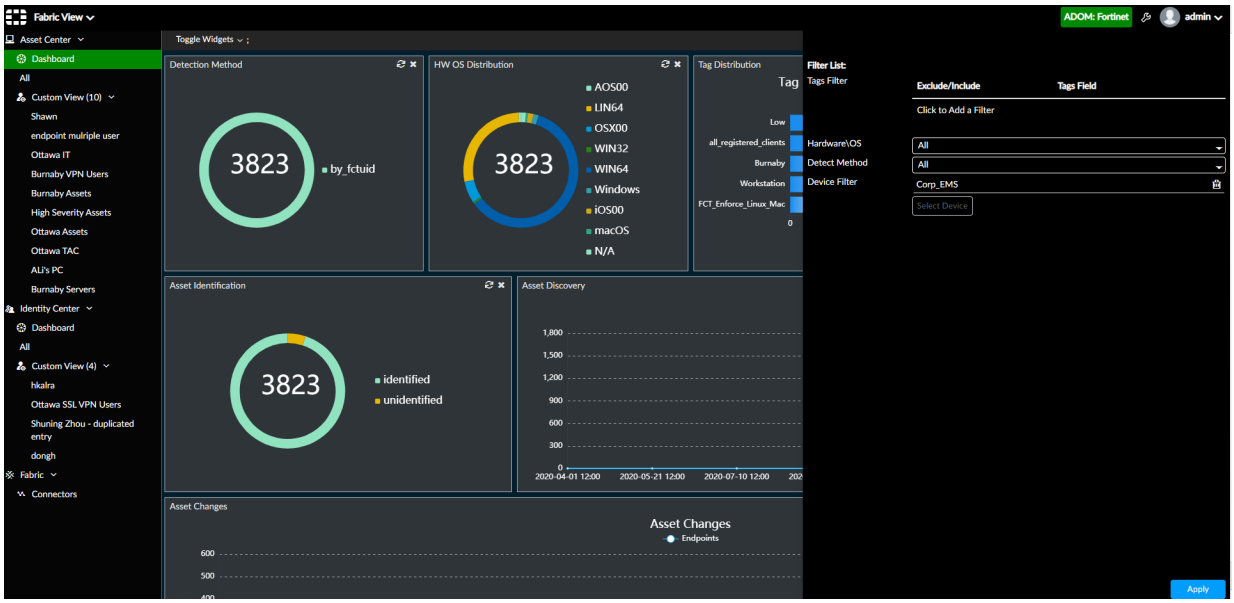
To view asset and identity dashboards:

1. Go to *Fabric View* > *Asset Center* > *Dashboard*.
   The Asset Center dashboard is displayed including twelve widgets.

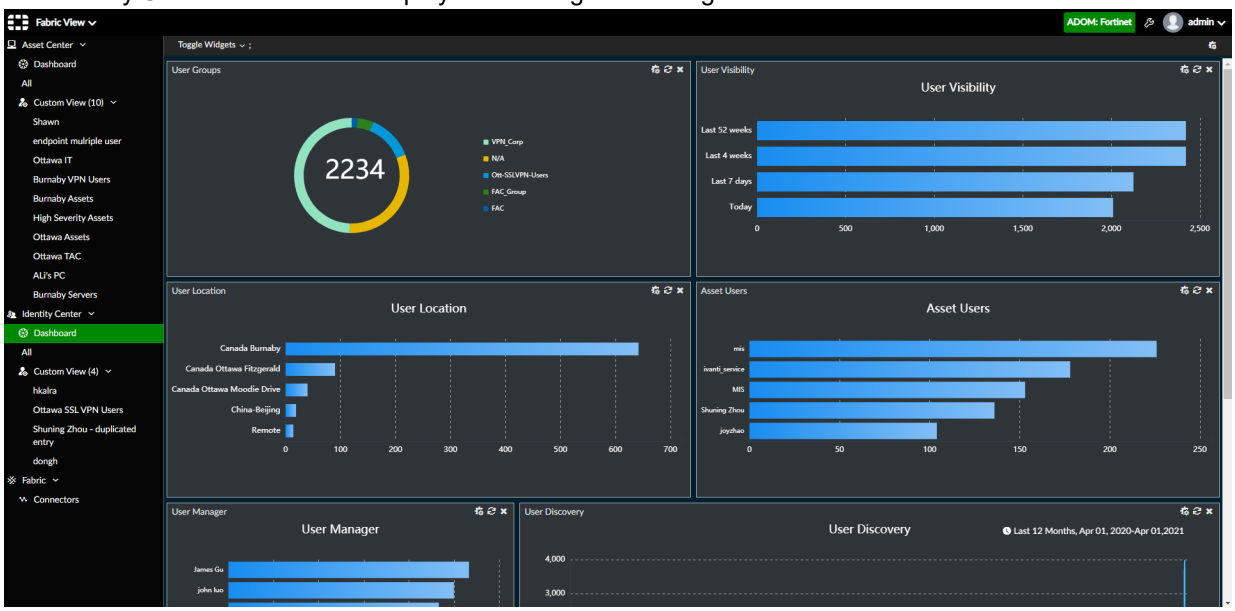
Click on the donut or bar charts to view drilldown results.

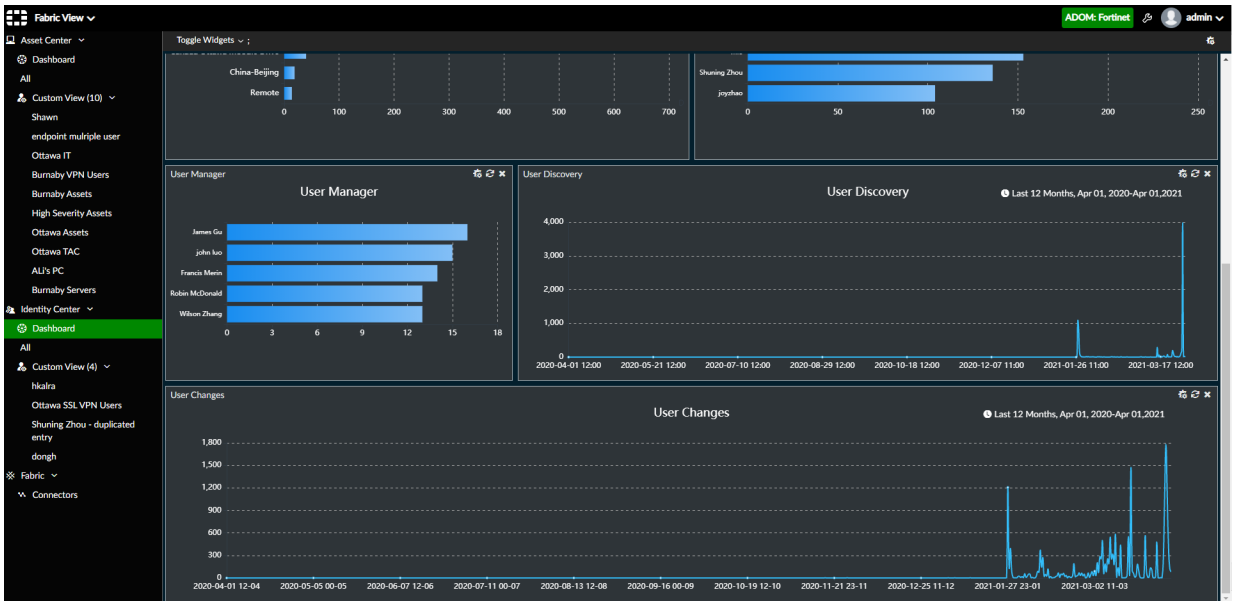


Click on the top-right filter icon to configure filters. For example, configure the filter to show endpoints from the device Corp_EMS.



2. Go to *Fabric View* > *Identity Center* > *Dashboard*.
The Identity Center dashboard is displayed including seven widgets about end users.




Fabric View
ADOM: Fortinet
admin
Asset Center
Dashboard
All
Custom View (10)
Shawn
endpoint mulriple user
Ottawa IT
Burnaby VPN Users
Burnaby Assets
High Severity Assets
Ottawa Assets
Ottawa TAC
ALi's PC
Burnaby Servers
Identity Center
Dashboard
All
Custom View (4)
hkalra
Ottawa SSL VPN Users
Shuning Zhou - duplicated entry
dongh
Fabric
Connectors
Toggle Widgets
China-Beijing
Remote
Shuning Zhou
joyzhao
User Manager
User Manager
James Gu
john luo
Francis Merin
Robin McDonald
Wilson Zhang
User Discovery
User Discovery
Last 12 Months, Apr 01, 2020-Apr 01,2021
User Changes
User Changes
Last 12 Months, Apr 01, 2020-Apr 01,2021

Log and Report

This section lists the new features added to FortiAnalyzer for logs and reports:

Logging

This section lists the new features added to FortiAnalyzer for logging:

Improve log forwarding bandwidth efficiency

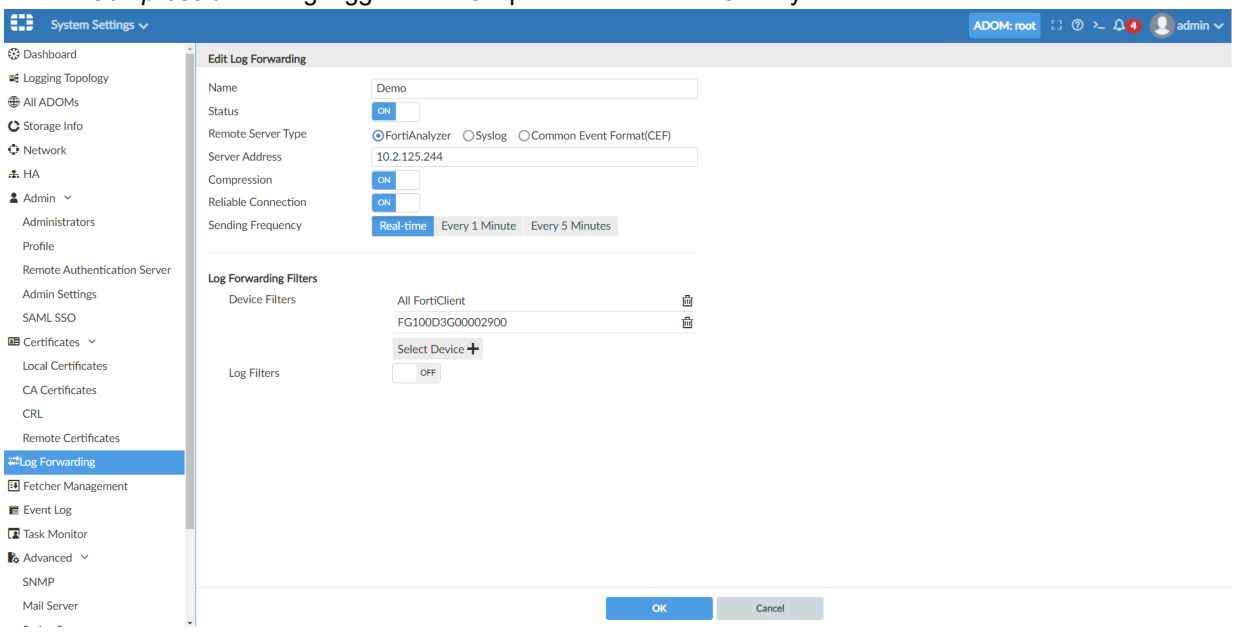
FortiAnalyzer supports a new option to allow log data to be compressed for bandwidth optimization when forwarding the logs to a remote server in FortiAnalyzer format.

Log messages will be compressed when this feature is enabled and both FortiAnalyzer devices support the log compression feature. When log forwarding is configured with compression enabled to a remote FortiAnalyzer that does not support compression, the logs will remain uncompressed.

To enable compression in log forwarding:

1. Go to *System Settings* > *Log Forwarding*, and click *Create New*.
2. Select *FortiAnalyzer* as the *Remote Server Type*, and configure the server settings for your remote FortiAnalyzer.

3. Set the *Compression* setting toggle to the *ON* position. It is set to *OFF* by default.



4. Click *OK* to save the log forwarding configuration.

Configuring log compression in the CLI

The following CLI setting has been added for log compression:

```
# set fwd-compression {enable|disable}
```

Following is an example of log forward configuration in the CLI:

```
config system log-forward
   edit 3
      set mode forwarding
      set fwd-max-delay realtime
      set server-name "demo"
      set server-addr "10.2.125.244"
      set fwd-reliable enable
      set fwd-compression enable
      set sync-metadata sf-topology interface-role device endusr-avatar
      set signature 6723252594909515930
   next
end
```

Diagnosing log forward compression

The log format is displayed in `diagnose test application logfwd 3` and the compression ratio is displayed with `diagnose test application logfwd 4`.

To view the log format:

1. In the FortiAnalyzer CLI, enter the following command:

```
diagnose test application logfwd 3
```

The output will include information about the log format.

```
#2: 244 => FortiAnalyzer @ 10.2.125.244:514 token=715983816682025708 Reliable Running
     Updt=1610129597
tlvm-ver=2 logfwd-ver=1 logfmt=SiedLog compress
Grp=ld-244 Qid=21 Updt=1610129598 Hash=1.115f51236d8e2a20.0.0
- Dev-filter: FG100D3G00002901,FG100D3G00002900
```

To view the compression ratio:

1. In the FortiAnalyzer CLI, enter the following command:

   ```
   diagnose test application logfwd 4
   ```

   The output will include information about the compression ratio.

   ```
   ** Server#1: 244 ld-244 Qid=21 Connected bind: from 16m42s ago
   nmsg-sent=9978 nlog-sent=452083 send_timeout=0 send_err=1
   conn_err=9 msg_append_err=0 unreliable-errno=0
   nbytes-sent=22781160 compress-ratio=82.1%
   rate in last 5sec, 30sec, 60sec
   msg/sec: 6.0 6.0 5.9
   log/sec: 280.4 290.2 285.2
   ```

The remote analyzer with this feature displays received compressed forwarded logs in `diagnose test application oftpd 7`.

To view received compressed logs:

1. In the FortiAnalyzer CLI, enter the following command:

   ```
   diagnose test application oftpd 7
   ```

   The output will include information about received compressed logs within the *log-forward gen2 stats* section.

   ```
   FAZVM64 # diagnose test application oftpd 7
      Reliable logging stats:
         log=547 log(>4k)=36
      Reliable log-forward stats:
         log=0 log(>4k)=0 reg=0 ack=0 ack_back=0 thr=0 optcode_err=0
      Reliable log-forward gen2 stats:
         Connections:
            From FAZ-VMTM20009184 @ 10.2.125.245 sig.745f02f721e21529 Connected 5m22.181s
                 ago
               Pos=1610387635.768239362.24429530.7 tlvm-ver=2 last_recv=1610387153 n_
                    flushed=2457 n_compressed=2457
         Stats:
            add=1 del=0 replace=0
            inactive=0 expired=0
         Errors:
            conn=0 conn_info=0 discard=0
            epoll.add=0 epoll.del=0
            rcv_tlvm=0 rcv_oversize=0 parse_msg=0 build_resp=0
      Internal log-forward stats:
         queued=0 (max=2048) update=757 (now=759)
         errors
            fortilogd-not-running=0 no-init=0 socket=0 no-recv=0 unknown=0
      Internal-forward stats by source:
         dev-nonreliable : 0
         fwd-reliable : 2457
         fwd-nonreliable : 0
         dev-batch-upload : 0
   ```

```
fct-batch-upload : 0
dev-reliable : 0
fwd-reliable-unencrypted : 0
fwd-ha-isync : 0
fwd-ha-isync-ack : 0
dev-reliable-encrypted : 547
fna-upload : 0
faz-appevt : 0
fct-siem : 0
unknown : 0
```

Per-device log receiving rate limit

This feature adds the ability to set log rate limit per device to pause log insertion when the configured limit is exceeded. This is to prevent misconfigured devices from flooding FortiAnalyzer with unwanted data.

To configure per-device log receiving rates:

1. Go to the FortiAnalyzer CLI and use the following commands to see that log receiving rate limits are not currently set:

   ```
   FAZ3000F # config system log ratelimit
   (ratelimit)# get
   mode : disable
   (ratelimit)#
   ```

   Enter the following command to view the current logging rates for each device:

   ```
   AZ3000F # diagnose test application fortilogd 17
   # device 1_minute 10_minute rate-limit dropped
   ------------------------------------------------------------------------
   1 FGT60E9982377487 34906.10 11800.36 0 0
   2 FG800D3915800008 1988.57 690.44 0 0
   3 FGHA000947503766_CID 0.00 0.00 0 0
   4 FGT51E3U16002689 0.47 0.17 0 0
   5 FWF61FTK19000247 45387.15 15514.16 0 0
   6 FAC-VM0000000000 0.00 0.00 0 0
   7 SYSLOG-AC105101 0.00 0.00 0 0
   8 FG140P3G13800040 12895.43 4495.17 0 0
   9 FGT60E9982377480 34906.83 11805.59 0 0
   10 FG280P4614800414 0.07 0.01 0 0
   11 FG101FTK19006708 9785.22 3177.97 0 0
   12 FL-3KF3R16000142 0.00 0.00 0 0
   13 FL3K5F3M15000004 0.02 0.01 0 0
   14 FGT40FTK20025663 19553.53 7087.56 0 0
   15 System 159423.38 54571.44 0 0
   ```

2. In the CLI, use the following commands to set the log receiving rate limit to manual and configure a new default rate limit:

   ```
   FAZ3000F # config system log ratelimit
   (ratelimit)# show
   config system log ratelimit
   set mode manual
   set device-ratelimit-default 1000
   end
   ```

   Enter the following command to view the updated default rate limit applied to logging devices:

   ```
   FAZ3000F # diagnose test application fortilogd 17
   # device 1_minute 10_minute rate-limit dropped
   ```

```
-------------------------------------------------------------------
1 FGT60E9982377487 1000.18 20781.08 1000 6680050
2 FG800D3915800008 1000.82 1385.01 1000 210858
3 FGHA000947503766_CID 0.00 0.00 1000 0
4 FGT51E3U16002689 0.45 0.42 1000 0
5 FWF61FTK19000247 1000.48 27342.83 1000 6779154
6 FAC-VM0000000000 0.00 0.00 1000 0
7 SYSLOG-AC105101 0.00 0.00 1000 0
8 FG140P3G13800040 1001.70 7753.74 1000 484191
9 FGT60E9982377480 1000.03 20778.19 1000 6680607
10 FG280P4614800414 0.07 0.05 1000 0
11 FG101FTK19006708 1000.52 5558.64 1000 1253065
12 FL-3KF3R16000142 0.00 0.00 1000 0
13 FL3K5F3M15000004 0.03 0.02 1000 0
14 FGT40FTK20025663 1001.62 12567.55 1000 3140384
15 System 7005.90 96167.54 42000 25228309
```

3. In the CLI, use the following commands to configure a per-device log rate limit for your devices.
   In this example, the FortiGate device is configured with a 2000 rate limit and FortiWiFi 61F devices are configured with a 1500 rate limit using wildcard support.

```
FAZ3000F # config system log ratelimit
(ratelimit)# show
config system log ratelimit
set mode manual
config device
edit 1
set device "FGT60E9982377480"
set ratelimit 2000
next
edit 2
set device "FWF61F*"
set ratelimit 1500
next
end
set device-ratelimit-default 1000
end
```

   Enter the following command to view the updated log rate limits:

```
FAZ3000F # diagnose test application fortilogd 17
# device 1_minute 10_minute rate-limit dropped
-------------------------------------------------------------------
1 FGT60E9982377487 1000.12 1000.18 1000 128460813
2 FG800D3915800008 812.20 882.80 1000 3990480
3 FGT51E3U16002689 0.40 0.58 1000 0
4 FWF61FTK19000247 1501.23 1369.88 1500 48970326
5 FAC-VM0000000000 0.00 0.00 1000 0
6 SYSLOG-AC105101 0.00 0.00 1000 0
7 FG140P3G13800040 0.00 704.49 1000 2673191
8 FGT60E9982377480 2000.07 1100.19 2000 128984024
9 FG280P4614800414 0.07 0.06 1000 0
10 FG101FTK19006708 1000.92 914.34 1000 24125577
11 FL-3KF3R16000142 0.00 0.00 1000 0
12 FL3K5F3M15000004 0.02 0.02 1000 0
13 FGT40FTK20025663 1001.30 917.09 1000 34486937
14 System 7316.32 6889.65 42000 371691348
```

4. Check the alert messages in widget Alert Message console to view messages about when log rate limits are exceed and logs are dropped:

```
Time Message
```

```
Feb 25, 09:36:08 Device FGT60E0000000299 logs dropped due to exceed configured rate-
     limit 60 logs/sec.
Feb 25, 09:36:08 Device FGT60E0000000435 logs dropped due to exceed configured rate-
     limit 60 logs/sec.
Feb 25, 09:36:08 Device FGT60E0000000260 logs dropped due to exceed configured rate-
     limit 60 logs/sec.
Feb 25, 09:36:07 Device FGT40FTK20025663 log-rate limited due to exceed configured
     rate-limit 1000 logs/sec.
Feb 25, 09:36:07 Device FG101FTK19006708 log-rate limited due to exceed configured
     rate-limit 1000 logs/sec.
```

This information is also available in local event logs:

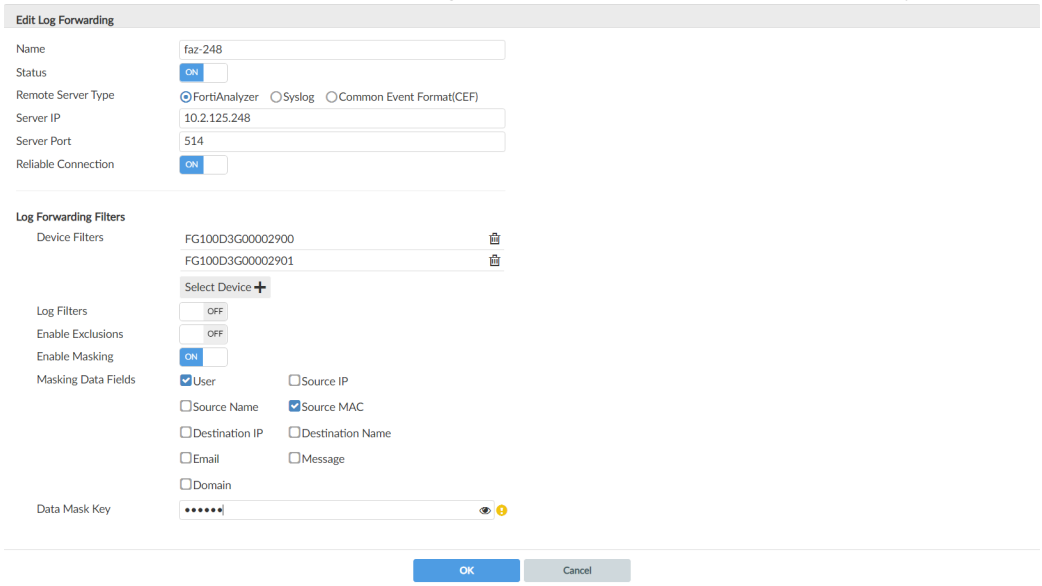
```
id=6933257507120873474 itime=2021-02-25 09:40:08 euid=1 epid=1 dsteuid=1 dstepid=1
     log_id=0030039002 subtype=logging type=event level=alert time=09:40:08
     date=2021-02-25 action=alert msg=Device FGT60E0000000121 logs dropped due to
     exceed configured rate-limit 60 logs/sec. desc=Log rate limit alert devid=FL-
     3KF3R16000142 devname=FL-3KF3R16000142 dtime=2021-02-25 09:40:08 itime_
     t=1614274808
id=6933257502825906182 itime=2021-02-25 09:40:07 euid=1 epid=1 dsteuid=1 dstepid=1
     log_id=0030039002 subtype=logging type=event level=alert time=09:40:07
     date=2021-02-25 action=alert msg=Device FWF61FTK19000247 log-rate limited due to
     exceed configured rate-limit 1500 logs/sec. desc=Log rate limit alert devid=FL-
     3KF3R16000142 devname=FL-3KF3R16000142 dtime=2021-02-25 09:40:07 itime_
     t=1614274807
```

Mask user data in log forwarder

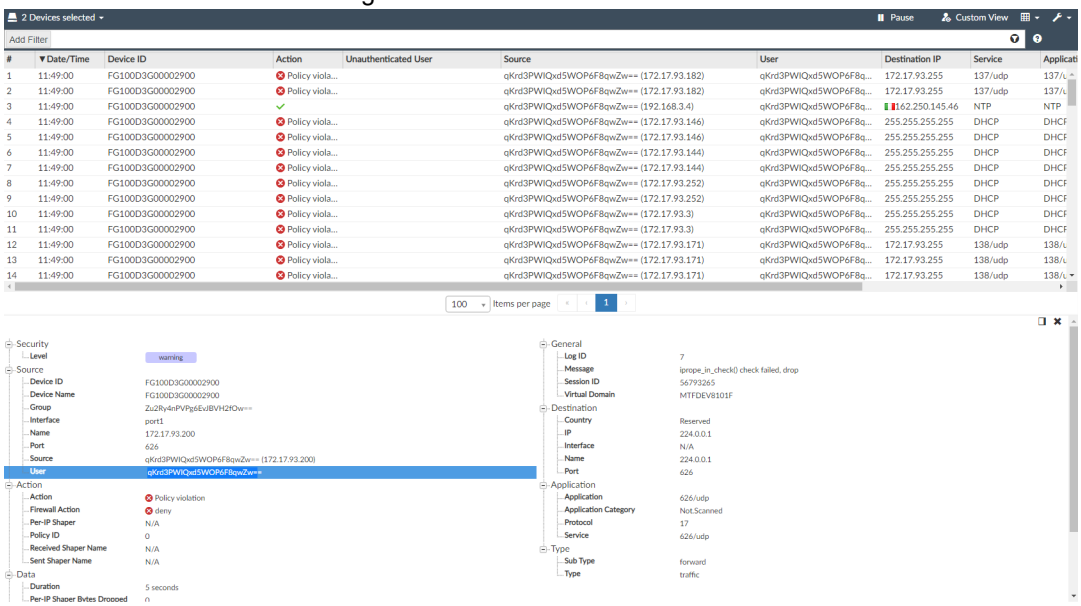
FortiAnalyzer includes an option to mask user privacy data when forwarding logs to a remote server in one of the supported types: FortiAnalyzer, Syslog, or CEF.

To configure data masking in log forwarding:

1. Go to *System Settings* > *Log Forwarding*, and configure a new or existing log forwarding profile.
2. Set the *Enable Masking* toggle to the *ON* position.
   Select the fields to be masked in *Masking Data Fields*, and create a *Data Mask Key*.



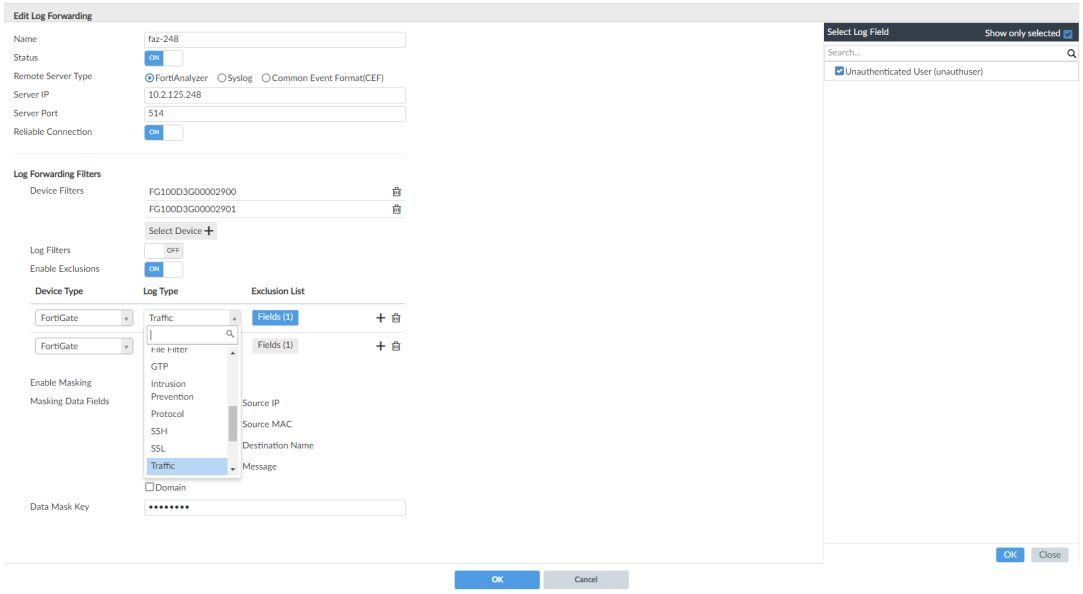
3. Click *OK* to save the log forwarding profile.
   The remote server will receive logs with the selected field values masked.



To configure log field exclusion in log forwarding:

1. Go to *System Settings* > *Log Forwarding*, and configure a new or existing log forwarding profile.

2. Set the *Enable Exclusions* toggle to the *ON* position.
   Add at least one log field to exclude.



3. Click *OK* to save the log forwarding profile.
   The remote server will receive logs with the selected log field removed.
   Log field exclusion will occur even when the same log field is also configured to be masked using data masking.

Configuring log field masking and exclusions in the CLI

The `log-field-exclusion-status` command was added to configure log field exclusions in the CLI.

The `log-masking-status` command was added to configure log field masking in the CLI.

The following is an example of the CLI used to configure log masking and exclusions:

```
config system log-forward
   edit 1
      set mode forwarding
      set fwd-max-delay realtime
      set server-name "faz-248"
      set server-ip "10.2.125.248"
      set fwd-reliable enable
      set sync-metadata sf-topology interface-role device endusr-avatar
         config device-filter
            edit 1
               set device "FG100D3G00002900"
            next
            edit 2
               set device "FG100D3G00002901"
            next
         end
      set signature 5899086158772996474
      set log-field-exclusion-status enable
         config log-field-exclusion
            edit 1
               set field-list "unauthuser"
            next
            edit 2
```

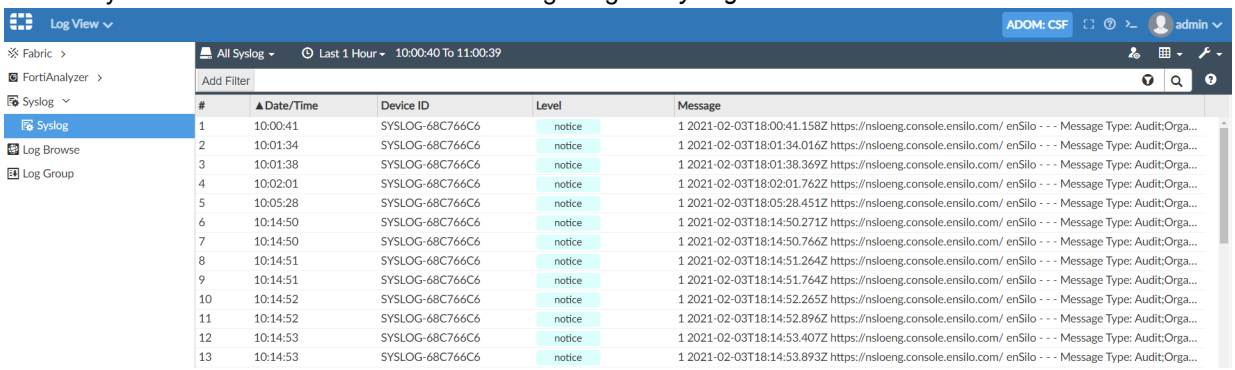
```
            set log-type ANY-TYPE
            set field-list "srcip"
        next
    end
    set log-masking-status enable
    set log-masking-fields user srcmac
    set log-masking-key ENC
        MTI0MDIwNDAxNDU4MzE3Nwt6SkhHfPMpmk5BN3cthOBoZwEvkjlBLEzBvUk89vcWnE0O6zRVadjlp9
        dPTJ8fw3svp1FF2uiPb5h6iN+Y0Y/be4sGO0J1TYVuMoyz5Od6xgmAFnG1M7F3QLNpXMp1COjD8MNR
        Ito
  next
end
```

FortiEDR Central Manager logging

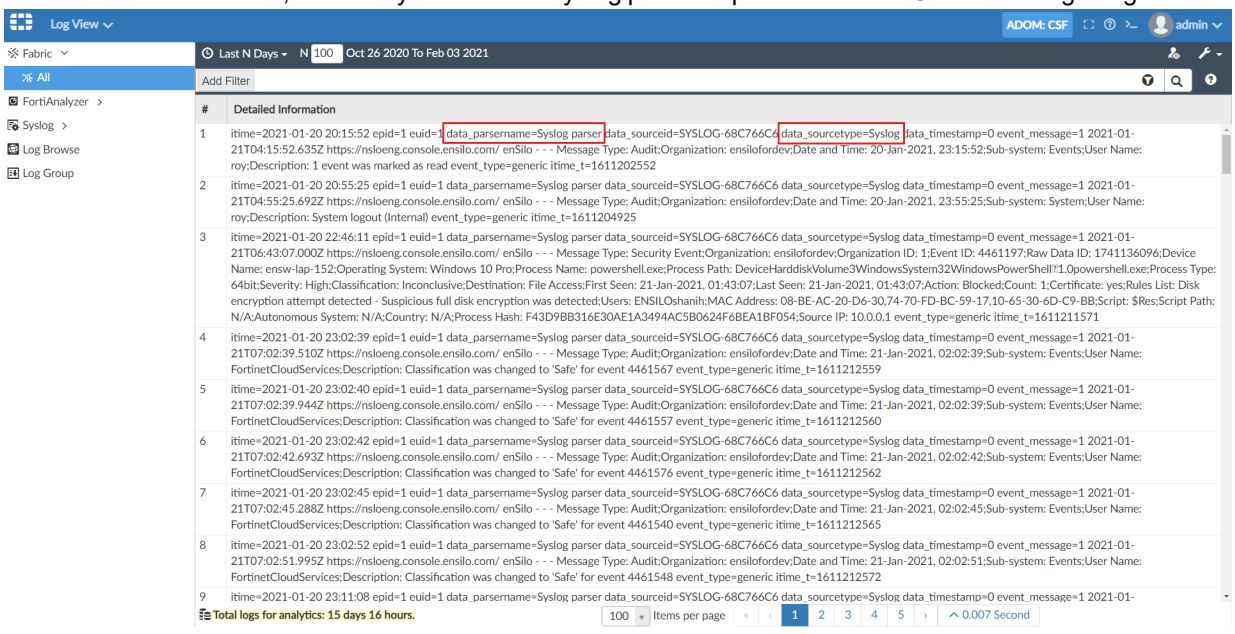
FortiEDR Central Manager can send its logs in Syslog format to FortiAnalyzer and the FortiAnalyzer parses the logs and inserts them into its SIEM database for event correlation and reporting.

To view FortiEDR logs in the Fabric log view:

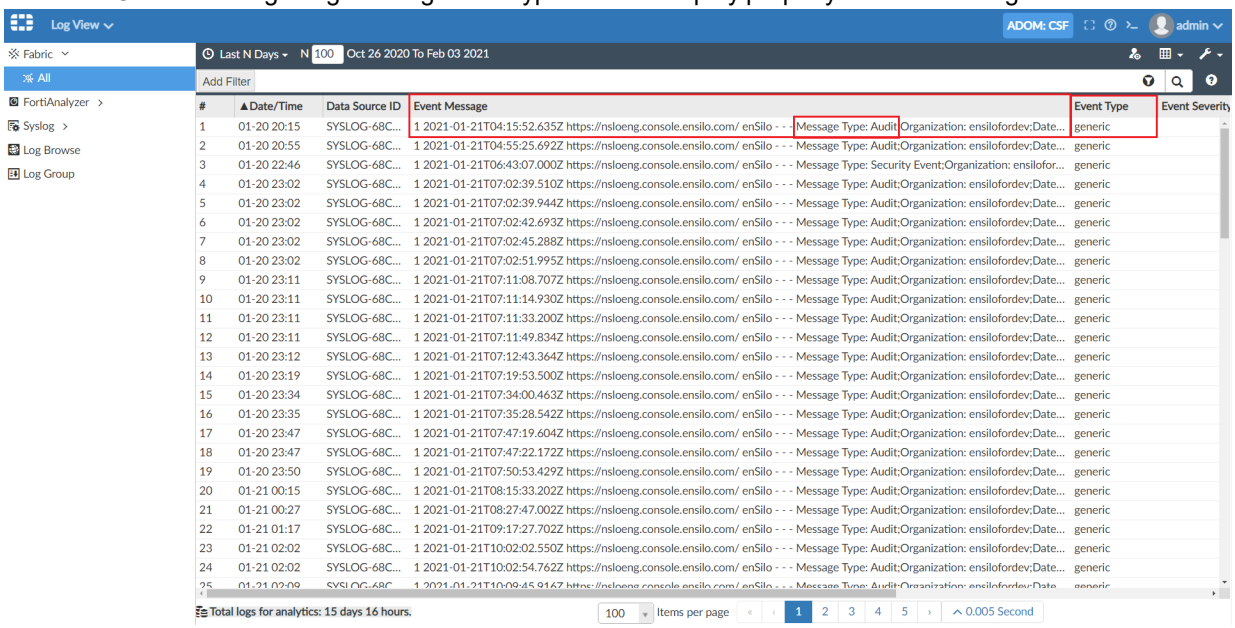
1. FortiAnalyzer can collect FortiEDR Central Manager logs in *Syslog*.



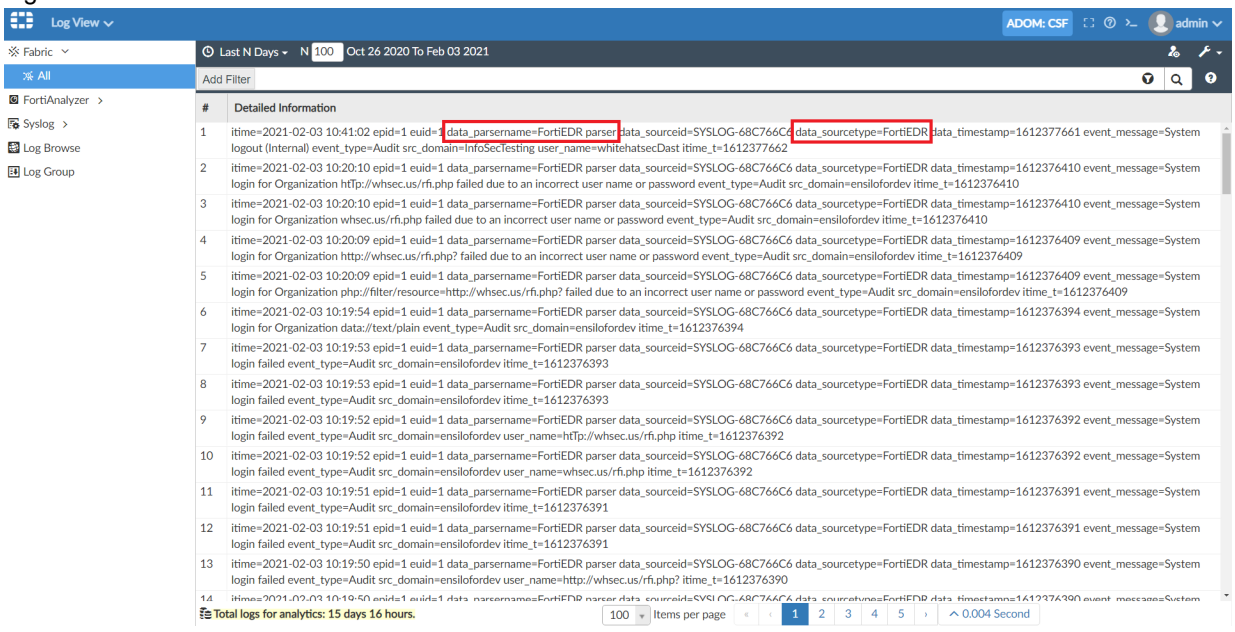
Before this enhancement, FortiAnalyzer uses the syslog parser to parse FortiEDR Central Manager logs in SIEM.



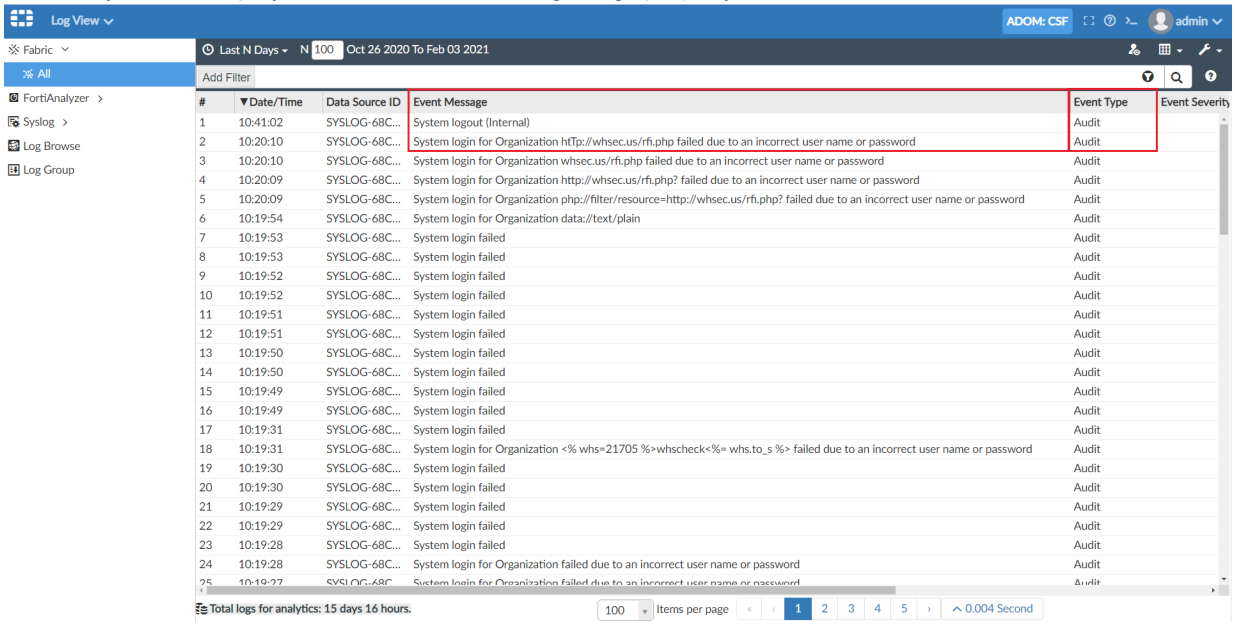
FortiEDR Central Manager log messages and types did not display properly in the Fabric log view.



2. After this enhancement, FortiAnalyzer includes a FortiEDR parser in the SIEM to parse FortiEDR Central Manager logs.



FortiAnalyzer can display FortiEDR Central Manager logs properly in the Fabric.



FortiAI logging on FortiAnalyzer - 7.0.1

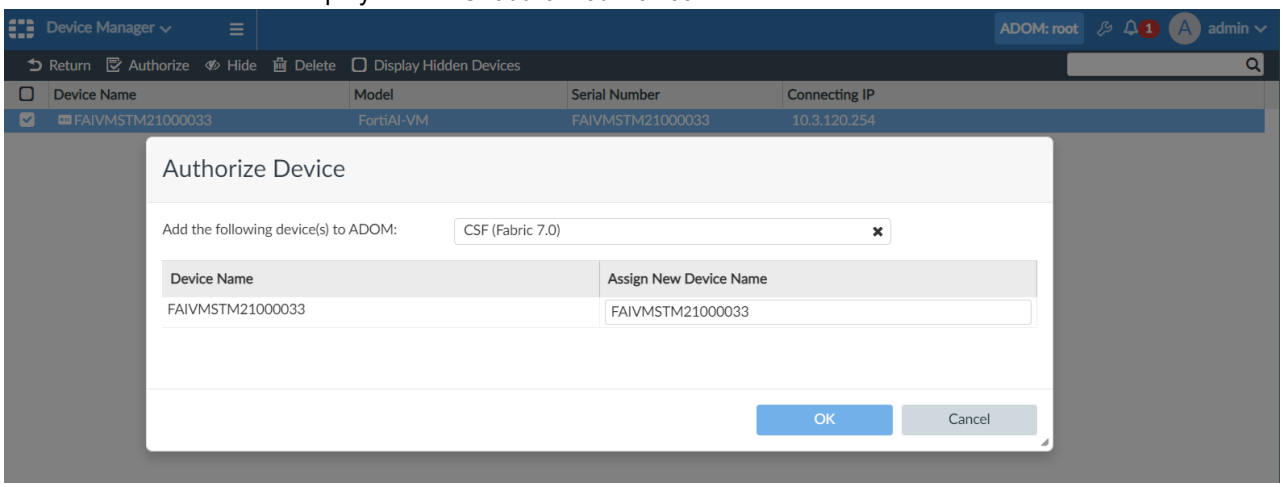
Starting in FortiAnalyzer 7.0.1, you can configure FortiAnalyzer to accept logs from a FortiAI device for use in the following ways:

- FortiAnalyzer can recognize FortiAi devices.
- FortiAI logs can be stored in Fabric ADOM.
- FortiAI can be viewed in LogView.
- FortiAI Device Type and Log Types are available in event handlers and report data sets.

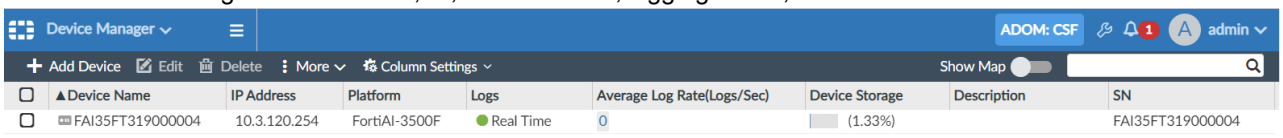
To add a FortiAI device to FortiAnalyzer:

1. On FortiAnalyzer, ensure you in are in the correct ADOM.
2. Go to *Device Manager* and add the FortiAI device.
   Previously, FortiAnalyzer could not recognize FortiAI devices. In 7.0.1 and later, FortiAnalyzer is able to recognize

the FortiAI device and will display it in the *Unauthorized Device* list once added.

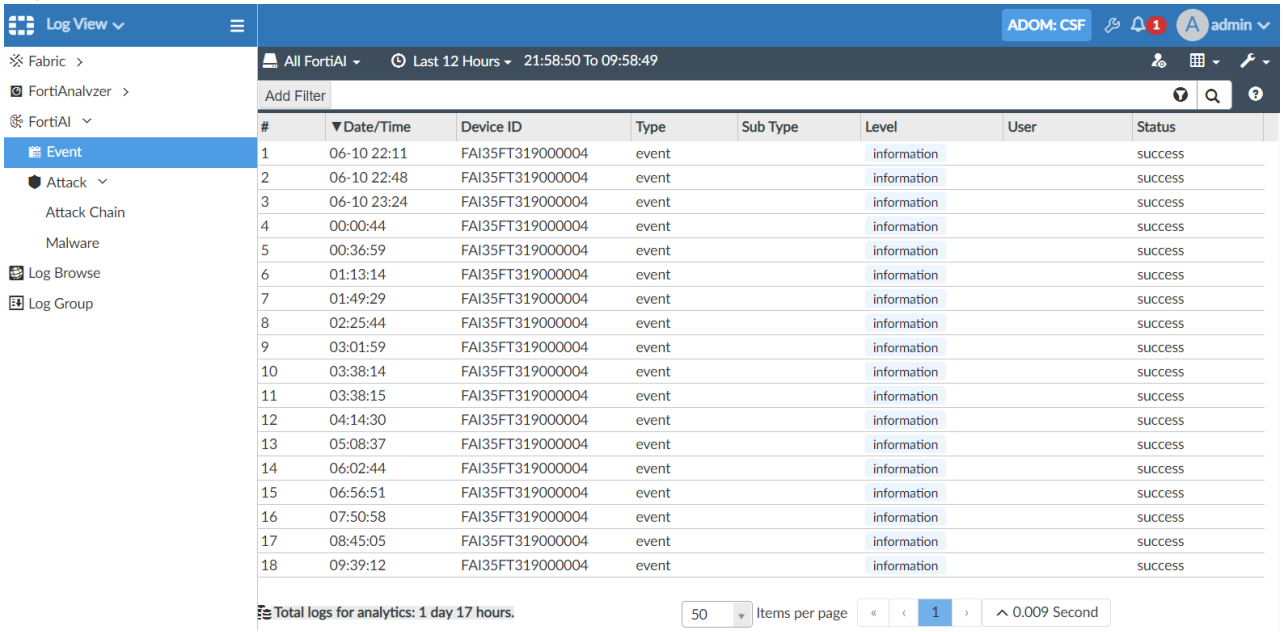


3. Select *Unauthorized Devices* and authorize the FortiAI device.
When the FortiAI device is authorized on FortiAnalyzer, it is listed in the FortiAnalyzer *Device Manager* with information including its device name, IP, serial number, logging status, etc.

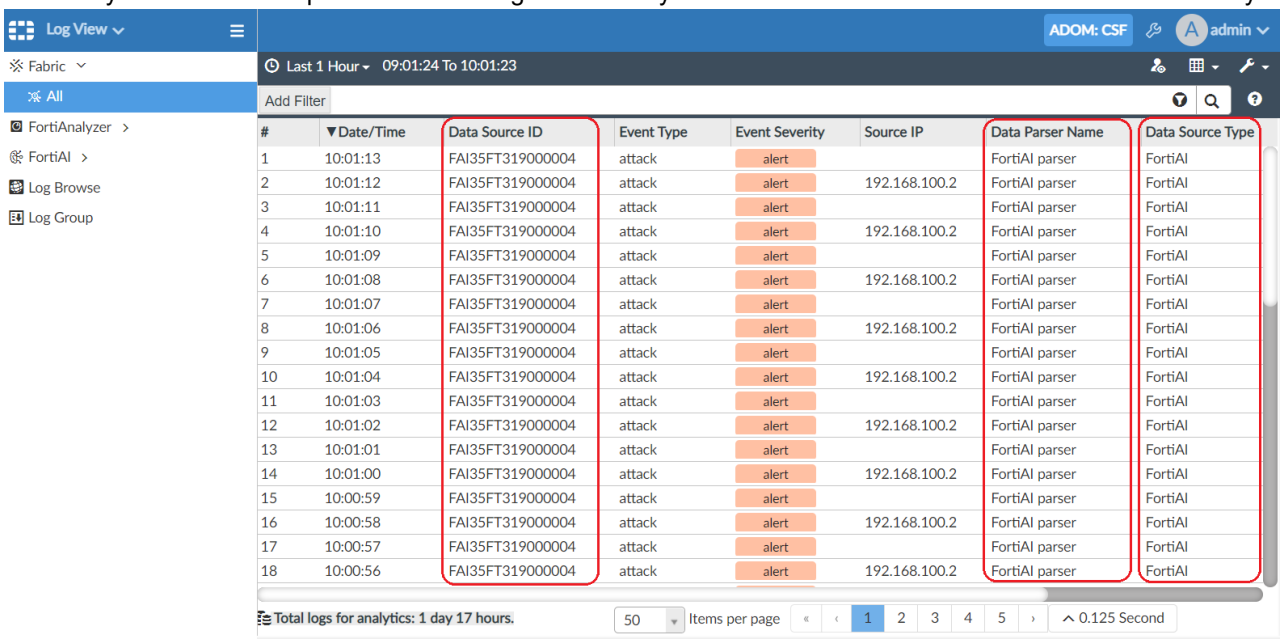


To view FortiAI logs in FortiAnalyzer:

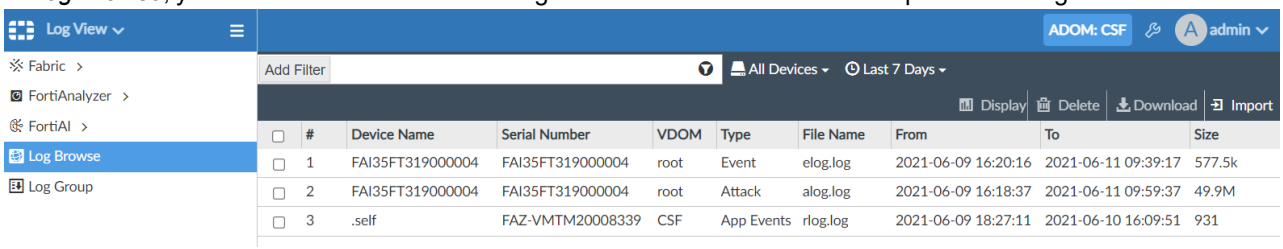
1. On FortiAnalyzer, ensure you are in the correct ADOM.
2. Go to *Log View* > *FortiAI*.
   There is a new *FortiAI* log type created for the FortiAI device. When FortiAI logs are received, they are displayed in *Log View*.



3. Go to *Log View* > *Fabric*.
   FortiAnalyzer adds a SIEM parser to FortiAI logs so that they can be viewed in the Fabric SIEM database correctly.

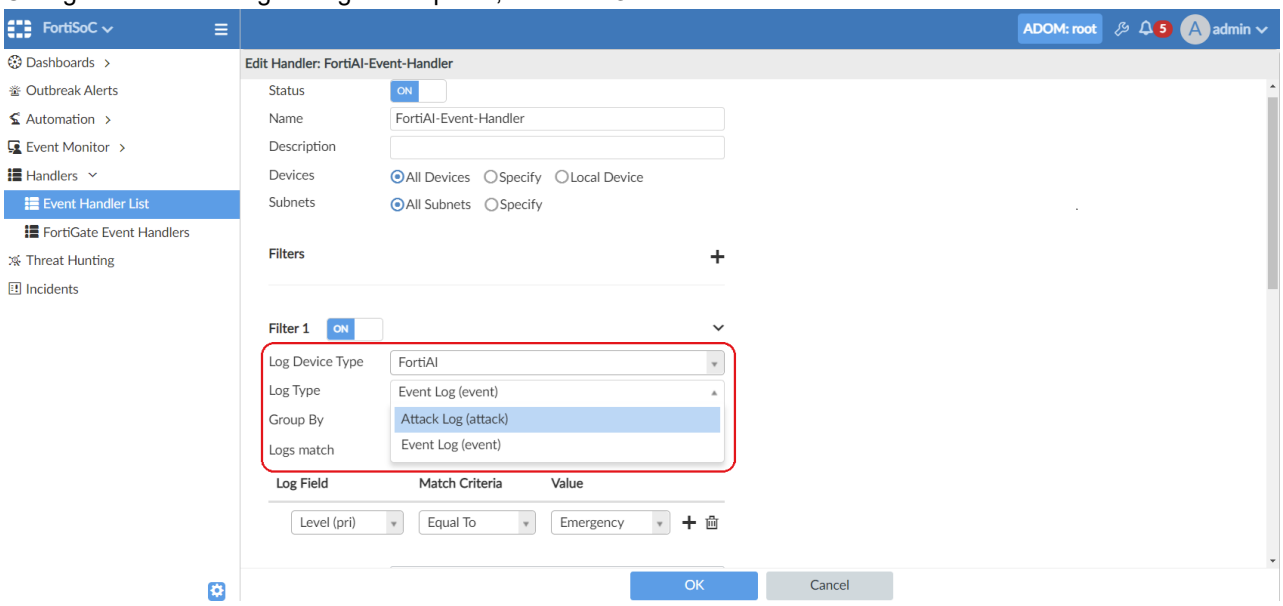


4. Go to *Log View* > *Log Browse*.
   In *Log Browse*, you can see the FortiAI device logs listed. You can download or import FortiAI logs.

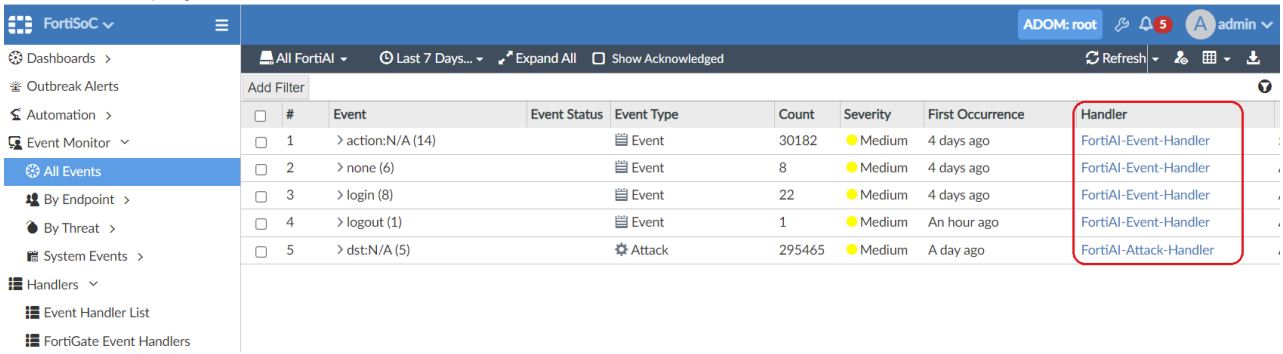


To create a custom event handler using FortiAI logs:

1. Go to *FortiSoC* > *Handlers* > *Event Handler List*, and create a new event handler.
2. Enter a name for the event handler, for example *FortiAI-Event-Handler*.
3. Enable a filter, and select *FortiAI* as the *Log Device Type*.
4. In *Log type*, select a FortiAI log type.
5. Configure the remaining settings as required, and click *OK* to save the event handler.

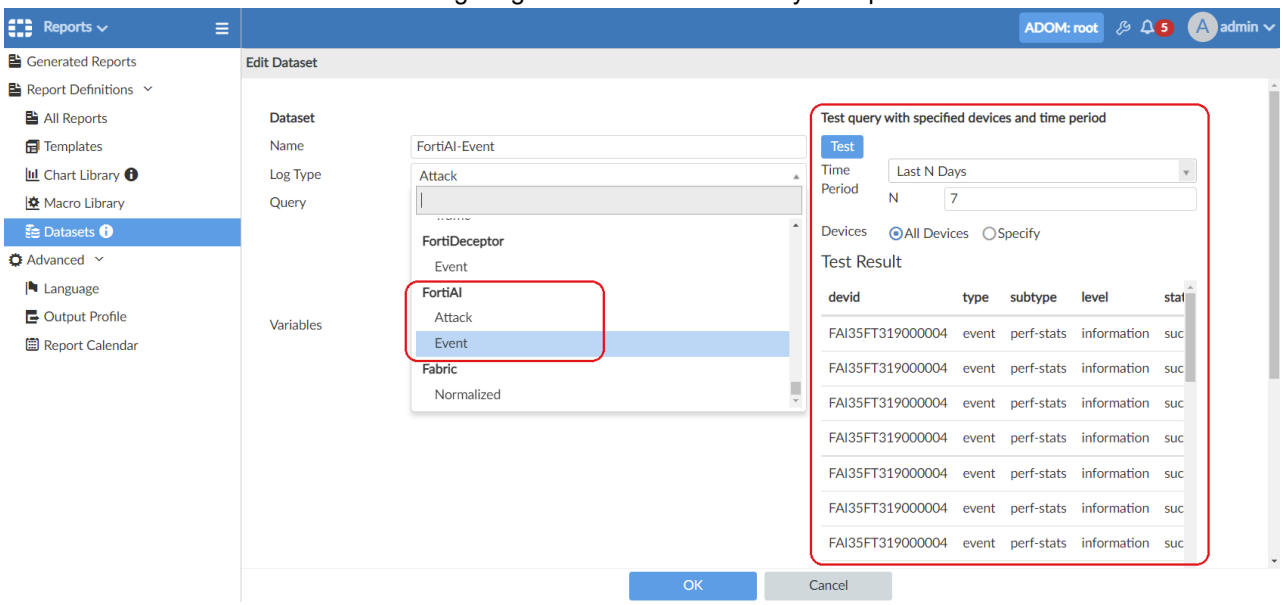


6. Events triggered by the event handler appear in *FortiSoC* > *Event Monitor* > *All Events*. The name of the event handler is displayed in the table.



To create a custom report using FortiAI logs:

1. Go to *Reports* > *Report Definitions* > *Datasets*, and create or edit a dataset.
2. Select a FortiAI log type in the Log Type dropdown.
3. Configure the remaining settings as required, and click *OK* to save the dataset.
   The dataset can now be used when configuring charts used in FortiAnalyzer reports.



Log forwarding enhancement - 7.0.1

With this feature enhancement, FortiAnalyzer log-forward-cache-size can set more than 80% system reserved space helping to prevent log loss.

When the cache is full, the latest logs are kept and older logs are dropped.

To configure the log forward cache size:

1. In the FortiAnalyzer CLI, enter the following commands to set the log forward cache size.
   In the following example, the cache size is set to *2000*.

```
config system global
   set log-forward-cache-size 2000
   Log-forward disk cache will be allocated from available disk quota and reserved
        space.
   All logs currently in log-forward disk cache will be dropped.
   Do you want to continue? (y/n)
```

2. In the CLI, enter the following command to see space usage:

```
diagnose log device
   Total Quota Summary:
      Total Quota Adom Allocated Logfwd Allocated Available Allocate%
      38140.9GB 32509.6GB 712.0GB(1000.0GB-288.0GB(reserved space)) 4919.3GB 87.1%
   System Storage Summary:
      Total Used Available Use%
      38500.9GB 26634.6GB 11866.4GB 69.2%
   Reserved space: 360.0GB ( 0.9% of total space, system reserved: 310.0GB,
        FortiRecorder disk quota: 50.0GB)
```

Reports

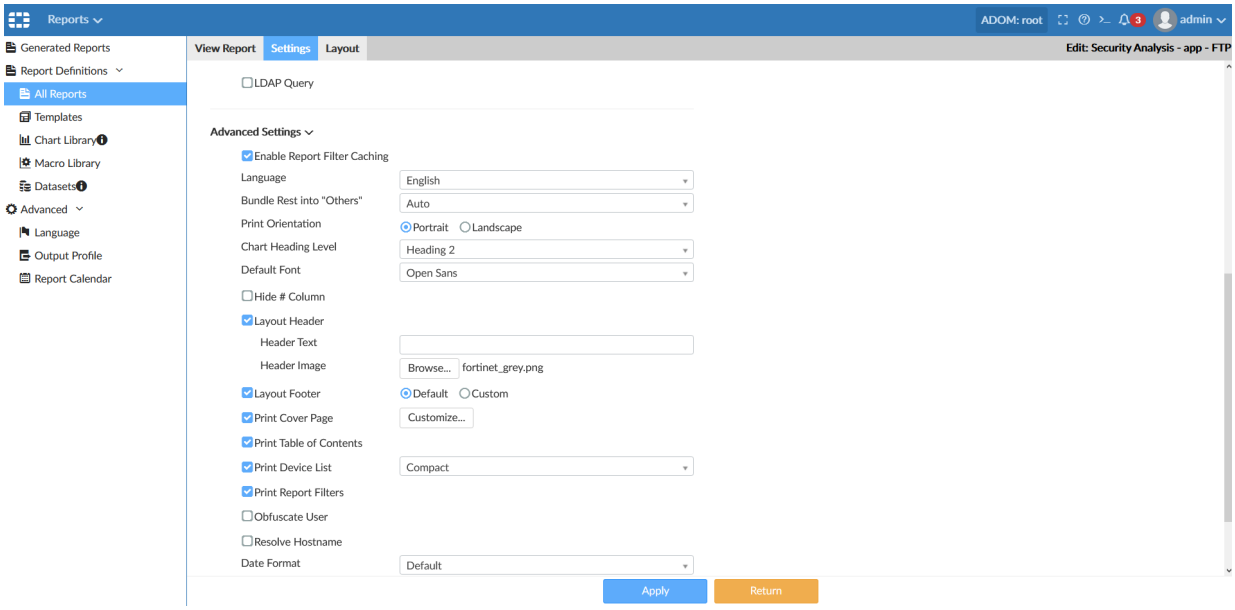
This section lists the new features added to FortiAnalyzer for reports:

Improved caching mechanism for reports

The report caching mechanism has been enhanced to improve processing speeds when generating multiple reports at the same time. When similar reports with different filters are processed at the same time, one hcache table is generated for all the reports in the queue.

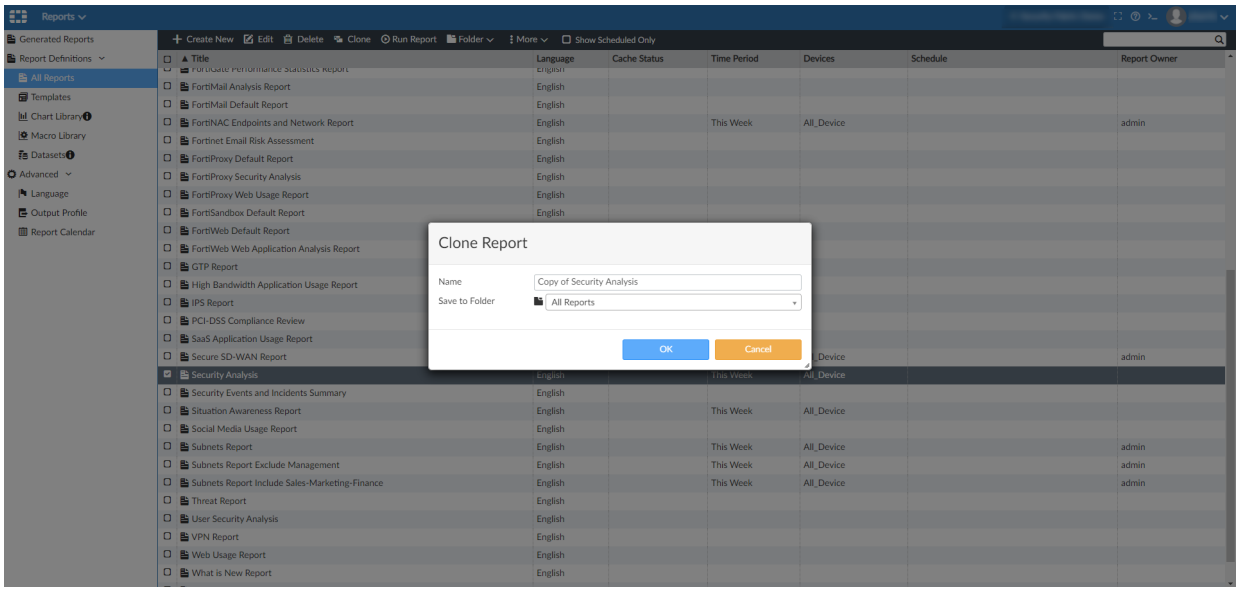
To run a report:

1. Go to *Reports* > *All Reports*, and select a report in the list.
2. Click *Settings* > *Advanced Settings* . *Enable Report Filter Caching*, is enabled by default.

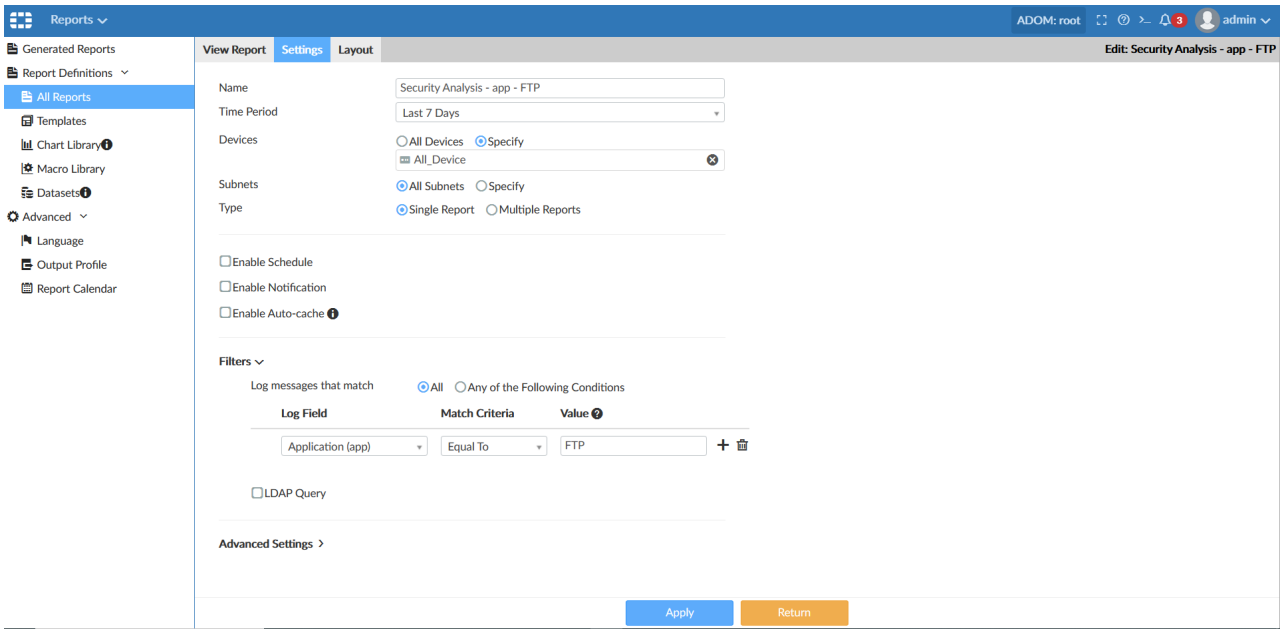


3. Click *Return*.

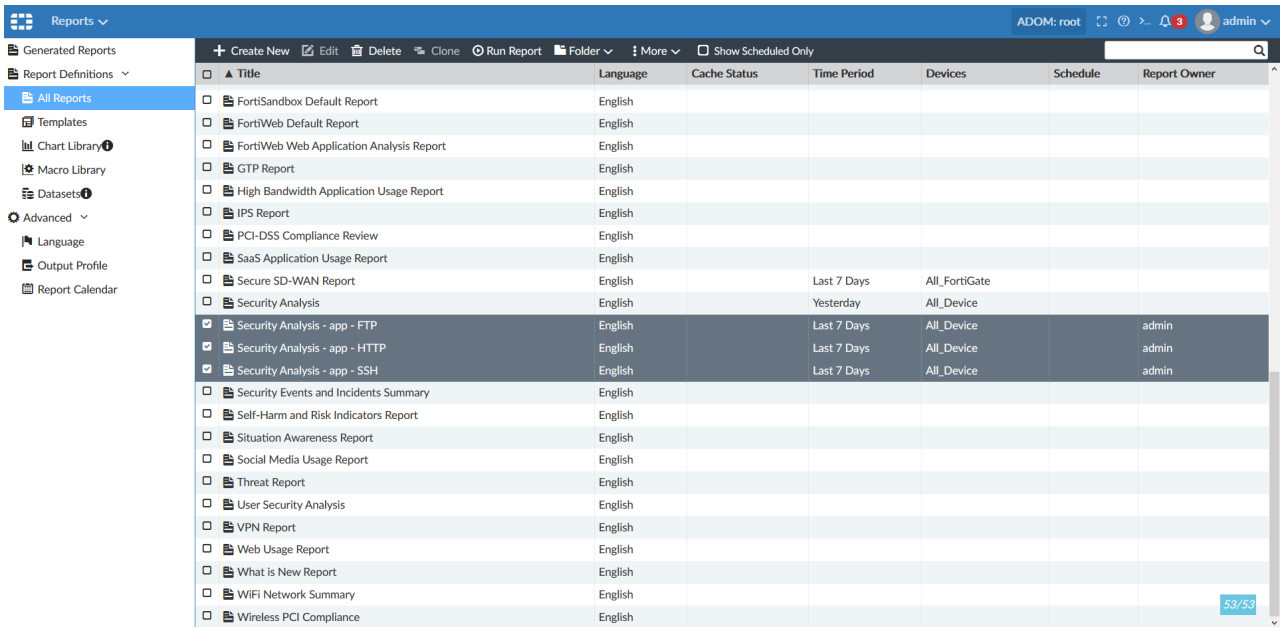
4. Clone the *Security Analysis Report*.



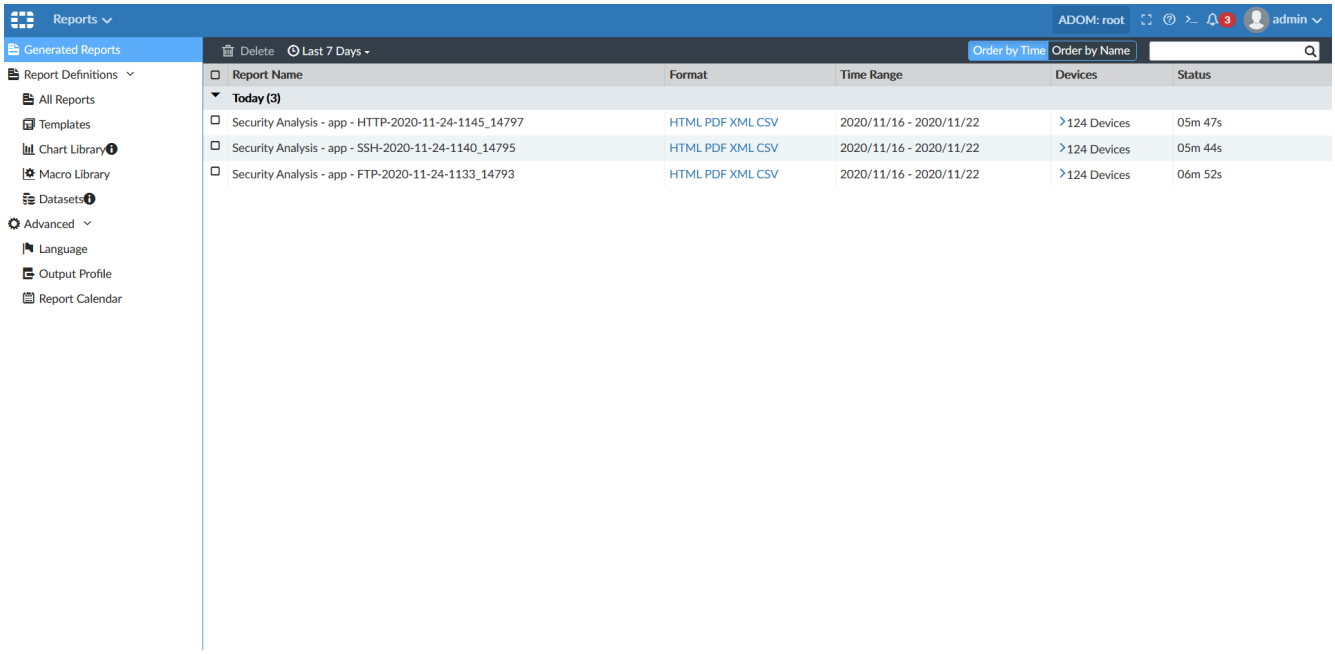
5. Apply different filter values to each copy of the report. For example *app=FTP*, *app=HTTP*, and *app=SSH*.



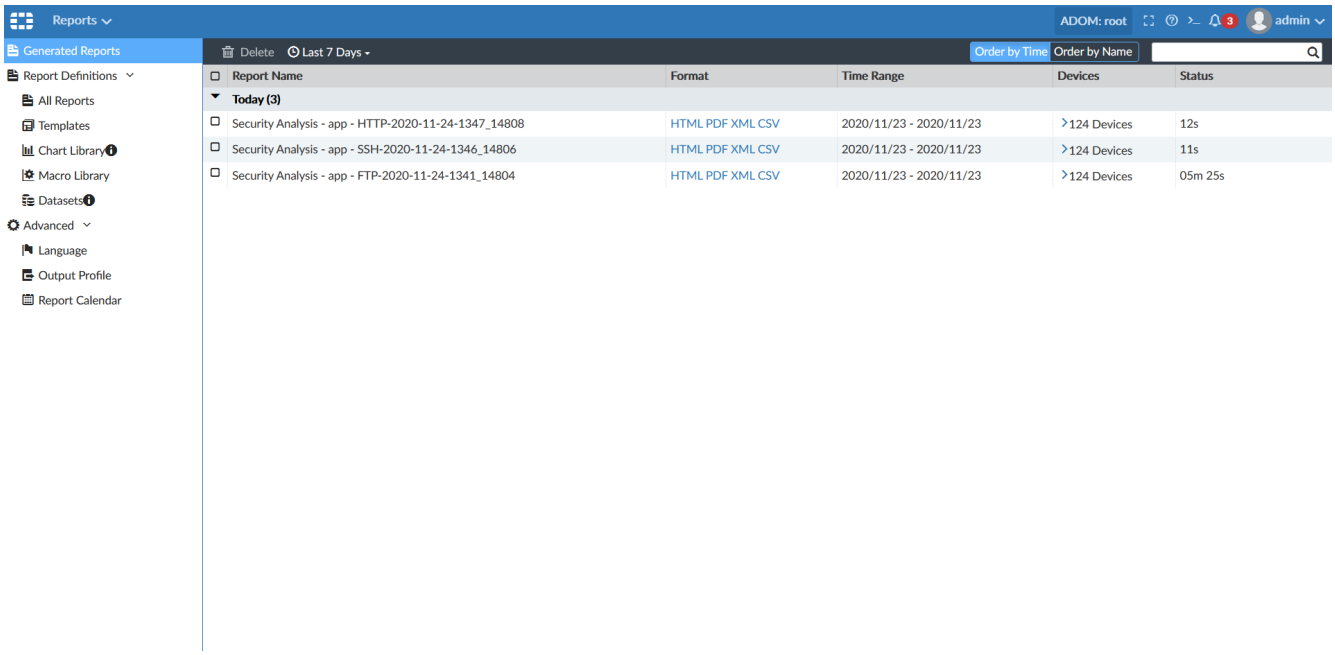
6. Select the cloned reports, and click *Run Report*.



Before these enhancements were implemented, it would take minutes to process multiple reports at the same time.



When *Enable Report Filter Caching* is enabled, it takes minutes to process the first report, while the processing time for subsequent reports is reduced to seconds.

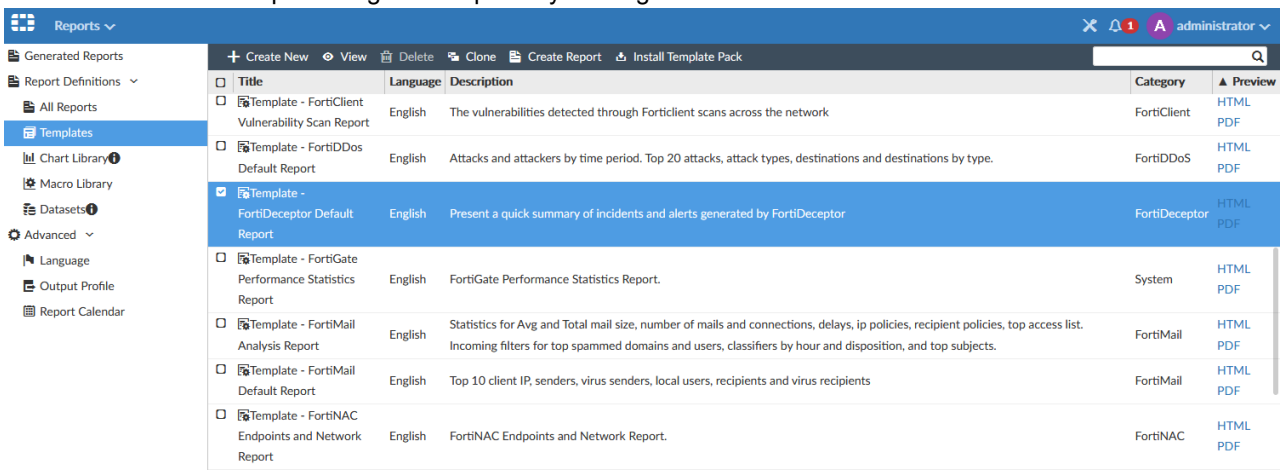


FortiDeceptor report

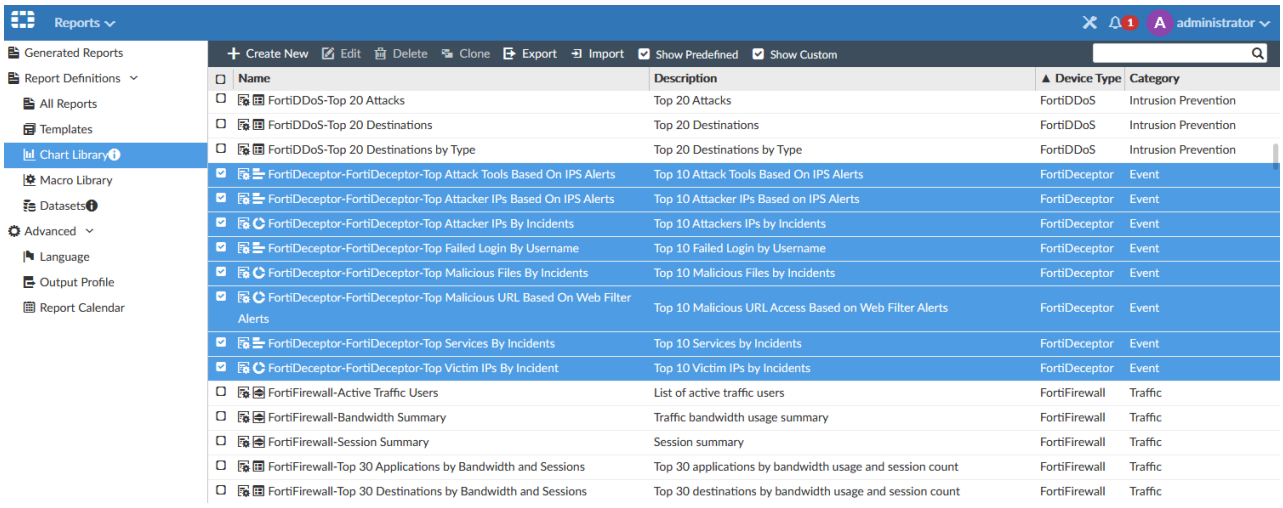
A new report template for FortiDeceptor has been added to FortiAnalyzer.

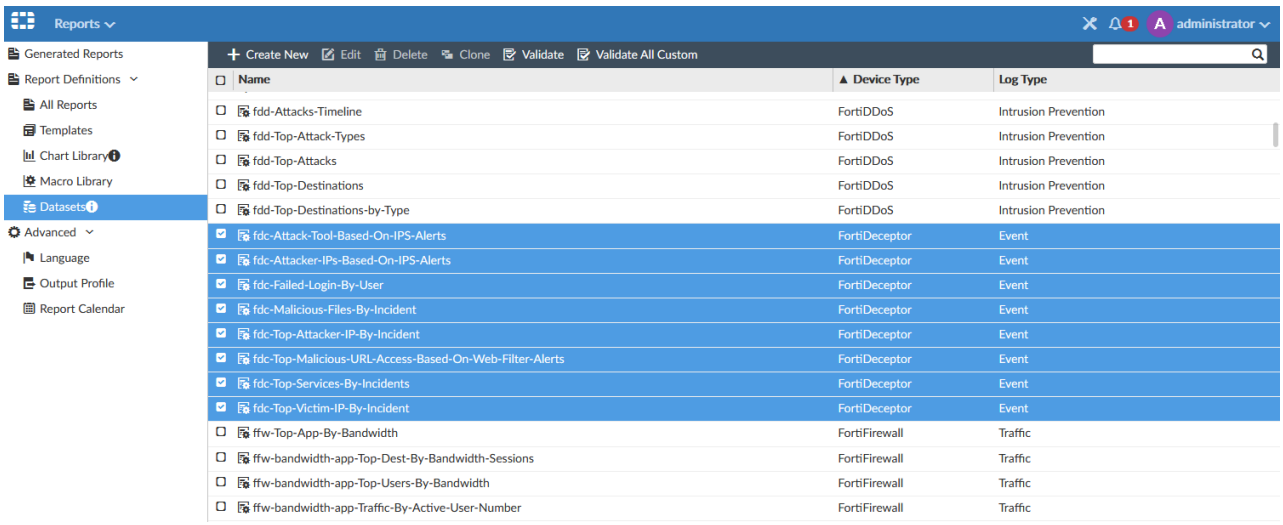
To view the FortiDeceptor report template:

1. Go to *Reports* > *Report Definitions* > *Templates*.
   Template - FortiDeceptor Default Report is available in the list of report templates, and you can click *HTML* or *PDF* in the *Preview* column to view a sample report.
   You can create a new report using this template by clicking *Create New*.



   The report template can be run or customized in the *All Reports* pane. A total of eight datasets and charts have been created to support the FortiDeceptor report, visible in *Chart Library* and *Datasets*.





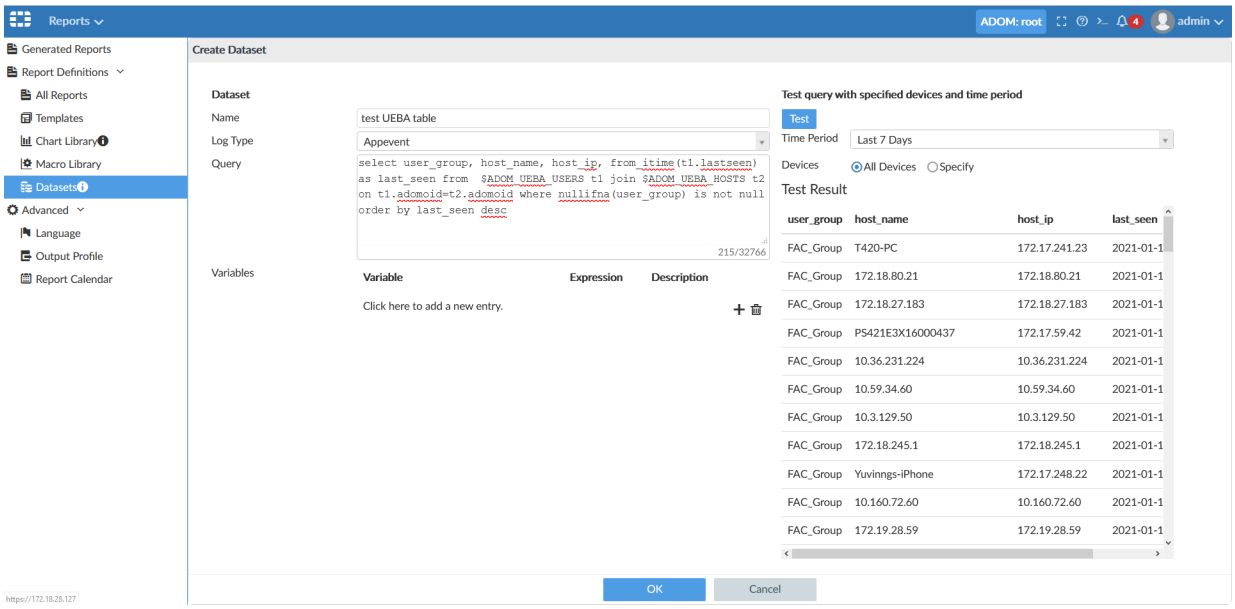
Central UEBA table for custom reporting and widgets

This is an enhancement to the current UEBA feature which enables users to query central UEBA tables by running custom report.

To create a report dataset based on the central UEBA table:

1. On FortiAnalyzer, go to *Reports* > *Report Definitions* > *Datasets*.
2. Click *Create New* to create a new dataset based on `$ADOM_UEBA_USERS` and `$ADOM_UEBA_HOSTS`.

3. Click *Test* to view test results.



4. Run a report based on the dataset. The report is generated successfully and contains information from the UEBA central table.

UEBA Central Table test

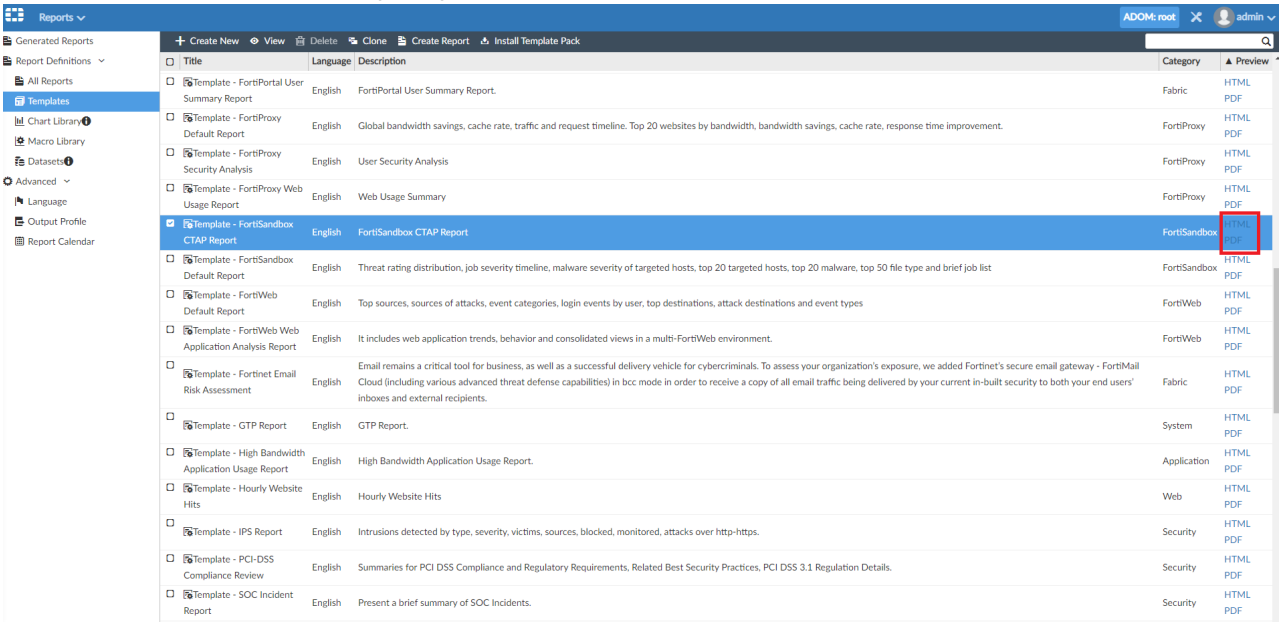
#	Client(Group)	host_name	host_ip	last_seen
1	FAC_Group	VAN-201520-PC	172.16.67.130	2021-01-15 12:07:33
2	FAC_Group	10.6.212.71	10.6.212.71	2021-01-15 12:07:33
3	FAC_Group	FortiFone FON-175	172.19.28.88	2021-01-15 12:07:33
4	FAC_Group	172.16.179.39	172.16.179.39	2021-01-15 12:07:33
5	FAC_Group	VAN-801156-LT	172.17.248.20	2021-01-15 12:07:33
6	FAC_Group	CentOs7-Uefi	172.17.70.176	2021-01-15 12:07:33
7	FAC_Group	172.16.196.252	172.16.196.252	2021-01-15 12:07:33
8	FAC_Group	172.16.197.57	172.16.197.57	2021-01-15 12:07:33
9	FAC_Group	LAPTOP-E1Q5SL04	172.16.199.19	2021-01-15 12:07:33
10	FAC_Group	VAN-200599-FP	172.16.62.71	2021-01-15 12:07:33
11	FAC_Group	172.18.78.163	172.18.78.163	2021-01-15 12:07:33
12	FAC_Group	172.18.69.110	172.18.69.110	2021-01-15 12:07:33
13	FAC_Group	172.17.74.136	172.17.74.136	2021-01-15 12:07:33
14	FAC_Group	FortiFone FON-175	172.19.28.89	2021-01-15 12:07:33
15	FAC_Group	172.17.217.10	172.17.217.10	2021-01-15 12:07:33
16	FAC_Group	172.18.74.159	172.18.74.159	2021-01-15 12:07:33
17	FAC_Group	172.16.199.228	172.16.199.228	2021-01-15 12:07:33
18	FAC_Group	Martin-iPhone	172.17.240.21	2021-01-15 12:07:33
19	FAC_Group	VAN-201290-KRSHN	172.16.63.101	2021-01-15 12:07:33
20	FAC_Group	172.16.97.25	172.16.97.25	2021-01-15 12:07:33
21	FAC_Group	172.16.99.5	172.16.99.5	2021-01-15 12:07:33
22	FAC_Group	172.17.61.173	172.17.61.173	2021-01-15 12:07:33
23	FAC_Group	VAN-201169-LT1	172.17.74.135	2021-01-15 12:07:33
24	FAC_Group	LG-Ericsson FON-460i	172.16.98.206	2021-01-15 12:07:33
25	FAC_Group	172.16.79.83	172.16.79.83	2021-01-15 12:07:33
26	FAC_Group	172.30.144.210	172.30.144.210	2021-01-15 12:07:33
27	FAC_Group	172.16.197.135	172.16.197.135	2021-01-15 12:07:33
28	FAC_Group	172.16.94.39	172.16.94.39	2021-01-15 12:07:33
29	FAC_Group	romeo-pc2	169.254.83.9	2021-01-15 12:07:33
30	FAC_Group	172.16.198.167	172.16.198.167	2021-01-15 12:07:33

FortiSandbox CTAP report

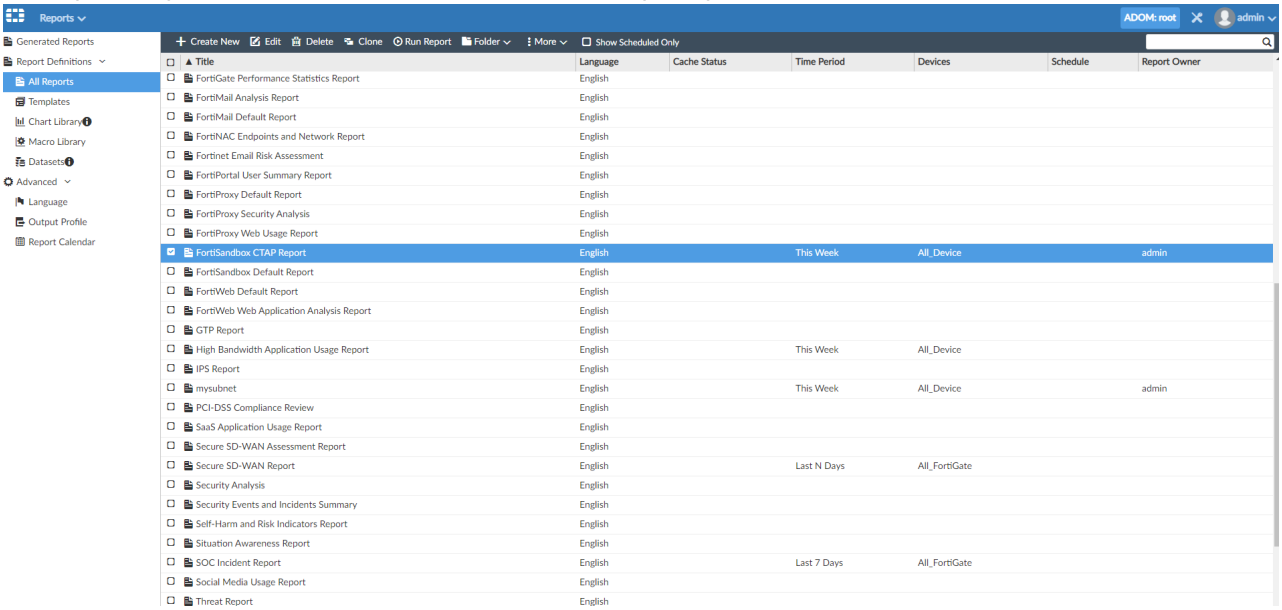
A new FortiSandbox report covers file scan statistics with detected incidents, malware, and targeted hosts.

To view the FortiSandbox CTAP report:

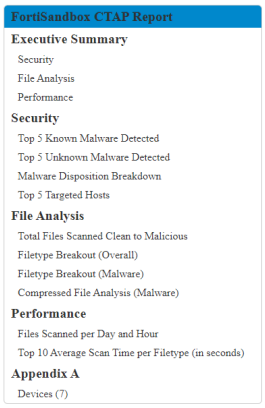
1. Go to Reports > Report Definitions > Templates.
   Template - FortiSandbox CTAP Report is available in the list of report templates, and you can click *HTML* or *PDF* in the *Preview* column to view a sample report.

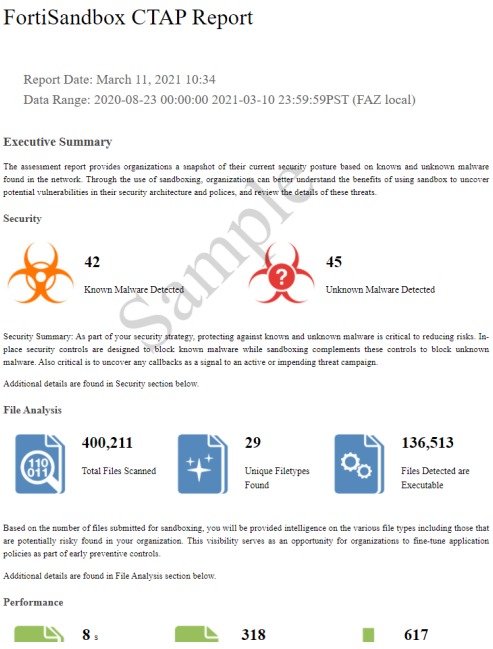


You can create a new report using this template by clicking *Create New*.
The report template can be run or customized in the *All Reports* pane.



Below is a sample of the information included with the FortiSandbox CTAP Report.




FortiSandbox CTAP Report

Report Date: March 11, 2021 10:34
Data Range: 2020-08-23 00:00:00 2021-03-10 23:59:59PST (FAZ local)

Executive Summary

The assessment report provides organizations a snapshot of their current security posture based on known and unknown malware found in the network. Through the use of sandboxing, organizations can better understand the benefits of using sandbox to uncover potential vulnerabilities in their security architecture and polices, and review the details of these threats.

Security

42 Known Malware Detected

45 Unknown Malware Detected

Security Summary: As part of your security strategy, protecting against known and unknown malware is critical to reducing risks. In-place security controls are designed to block known malware while sandboxing complements these controls to block unknown malware. Also critical is to uncover any callbacks as a signal to an active or impending threat campaign.

Additional details are found in Security section below.

File Analysis

400,211 Total Files Scanned

29 Unique Filetypes Found

136,513 Files Detected are Executable

Based on the number of files submitted for sandboxing, you will be provided intelligence on the various file types including those that are potentially risky found in your organization. This visibility serves as an opportunity for organizations to fine-tune application policies as part of early preventive controls.

Additional details are found in File Analysis section below.

Performance

8 s

318

617

Organize reports in folders

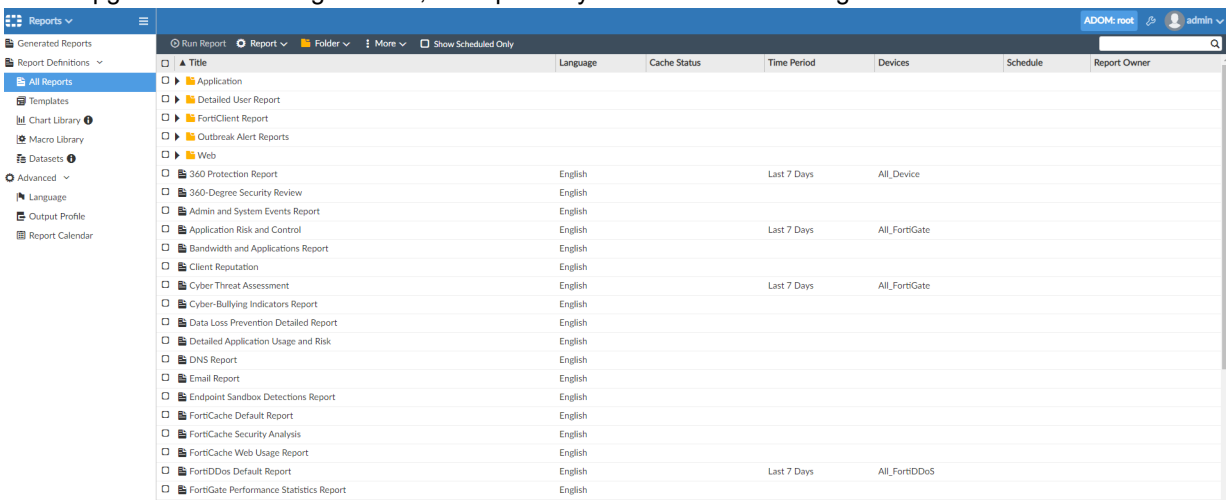
Reports are organized in folders and sorted per data sources and the areas of interest for consistency and better usability.

For all upgraded and existing ADOMs, the reports layout structure and configuration will remain the same as before.

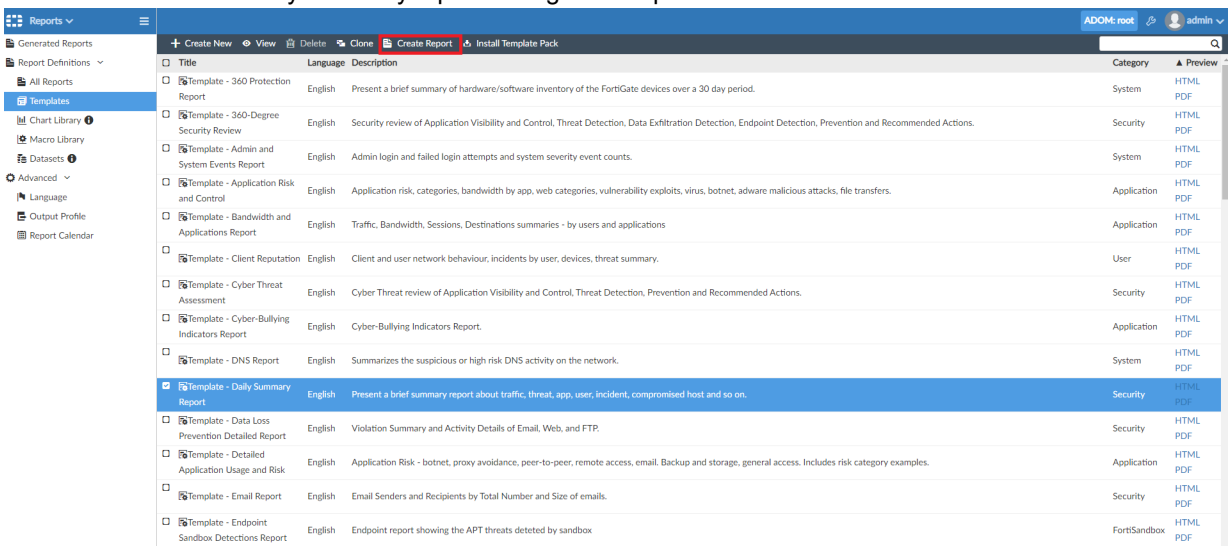
For newly created ADOMs, the reorganized folder structure feature is available. All reports, excluding the new Daily Summary Report, are sorted into folders by the report data sources and area of interest.

To view report folders :

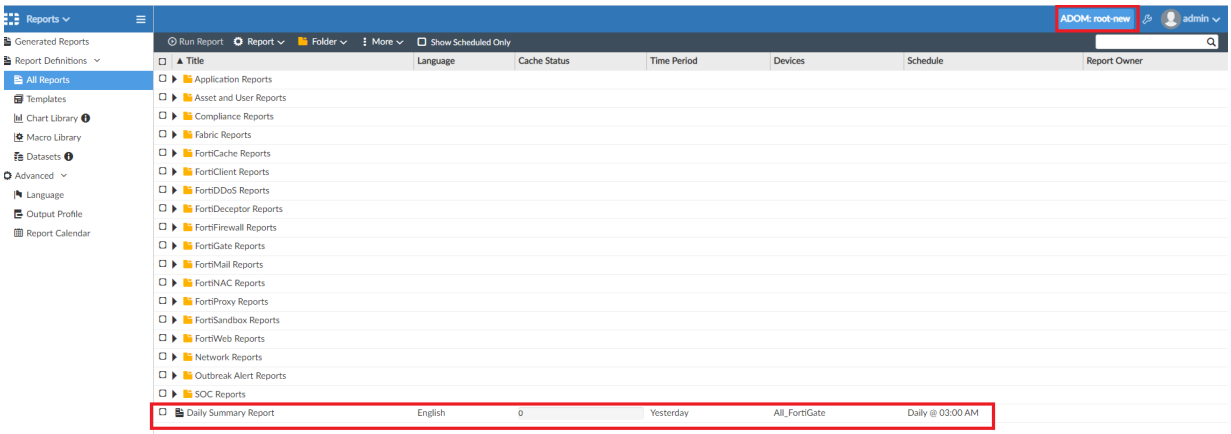
1. In an existing/upgraded ADOM, go to *Reports* > *Report Definitions* > *All Reports*.
   For all upgraded and existing ADOMs, the reports layout structure and configuration will remain the same as before.



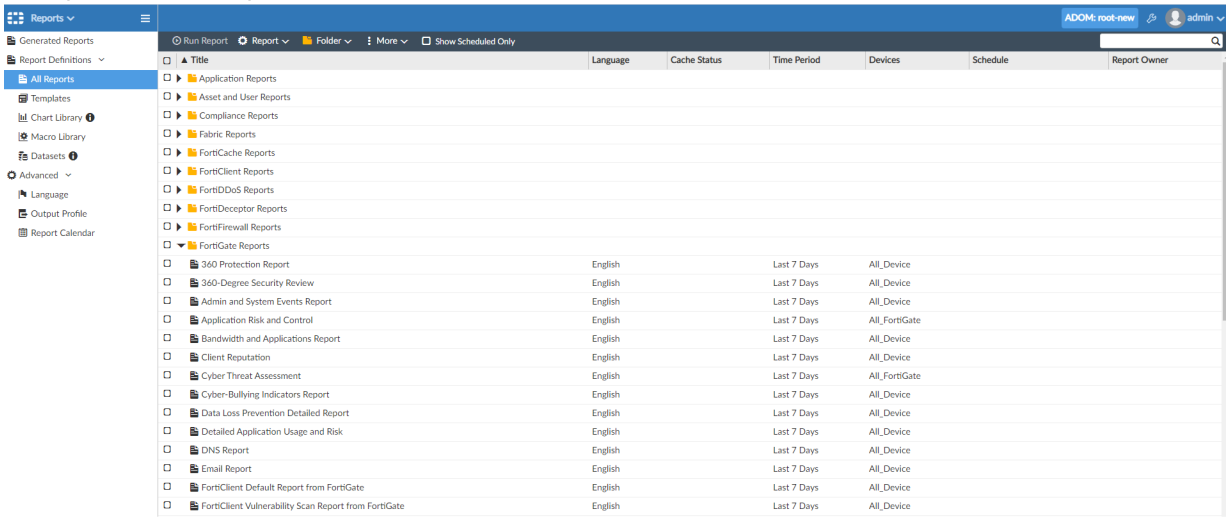
   A new *Daily Summary Report* template is available in upgraded Fabric and FortiGate ADOMs. Administrators can create and customize daily summary reports using this template.



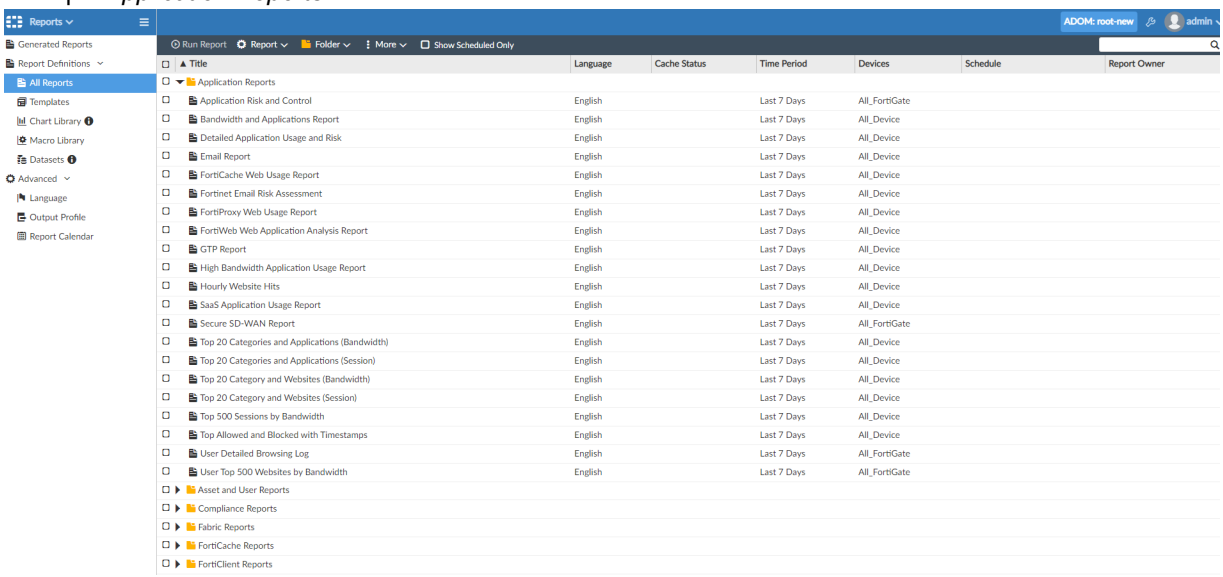
2. In a Fabric ADOM created in FortiAnalyzer 7.0.0, go to *Reports* > *Report Definitions* > *All Reports*.
   For newly created ADOMs, the reorganized folder structure feature is available. All reports, excluding the new Daily Summary Report, are sorted into folders by the report data sources and area of interest.



Expand a data source folder to view reports within that folder that have the same data source assigned to it, for example *FortiGate Reports*.

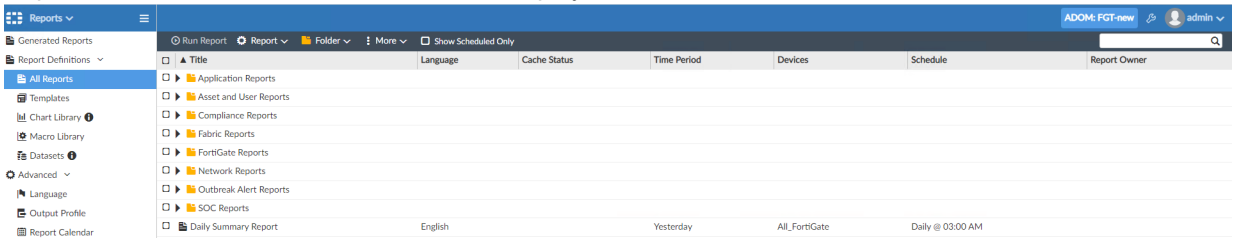


Expand an area of interest folder to view reports within that folder that belong to the same area of interest, for example *Application Reports*.

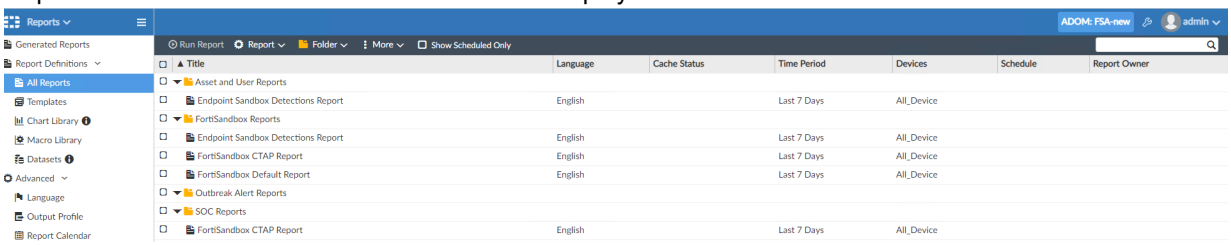


Reports that have mixed data sources are included in the *Fabric Reports* folder.

3. In a FortiGate ADOM created in FortiAnalyzer 7.0.0, go to *Reports* > *Report Definitions* > *All Reports*. Reports available in the FortiGate ADOM are displayed with the new folder structure.



4. In a FortiSandbox ADOM created in FortiAnalyzer 7.0.0, go to *Reports* > *Report Definitions* > *All Reports*. Reports available in the FortiSandbox ADOM are displayed with the new folder structure.

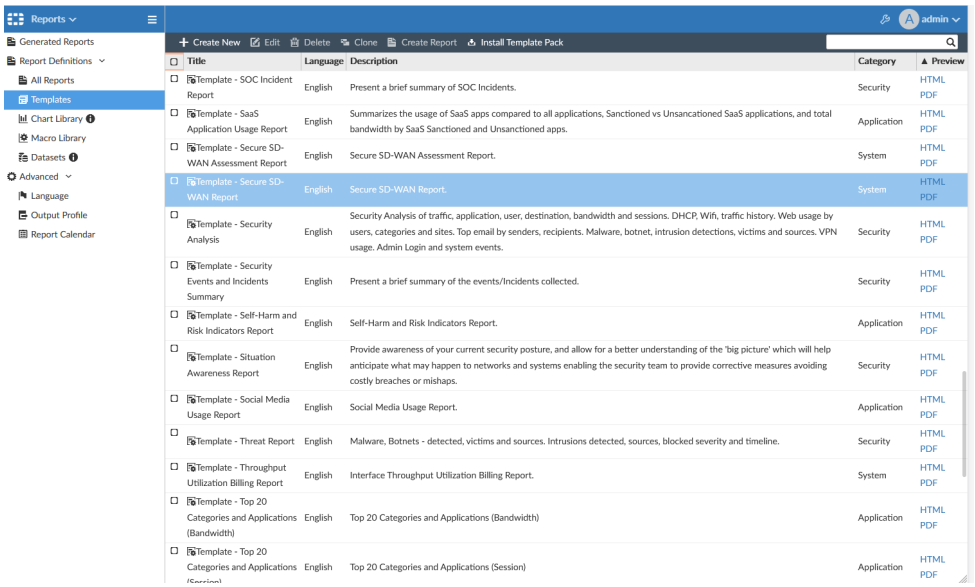


Additional charts for SD-WAN reporting - 7.0.1

The Secure SD-WAN Report now includes charts for SD-WAN Link Health Status and the Inbound/Outbound status per SD-WAN device interfaces.

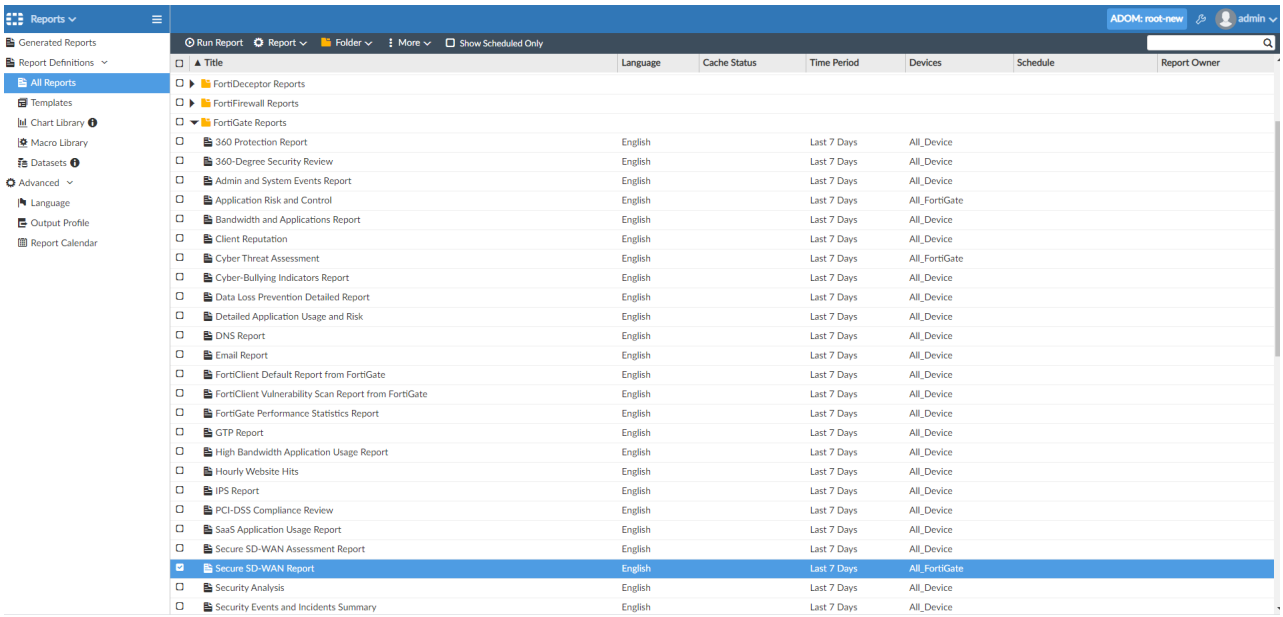
To view additional charts in the SD-WAN Report:

1. Go to *Reports* > *Templates*.
2. In the templates pane, right-click *Secure SD-WAN Report*, and click *Create Report*.

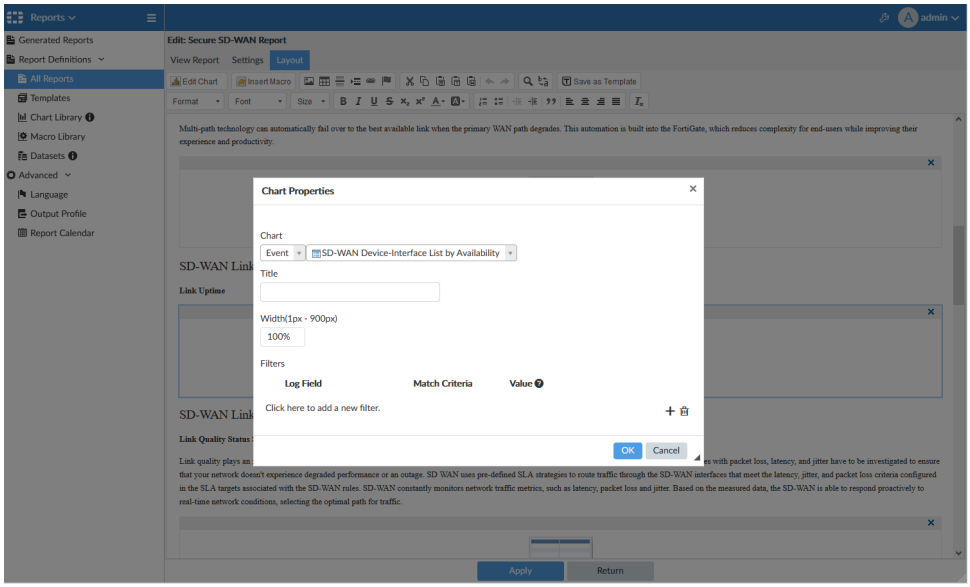


3. In the tree menu, click *Report Definitions* > *All Reports*.

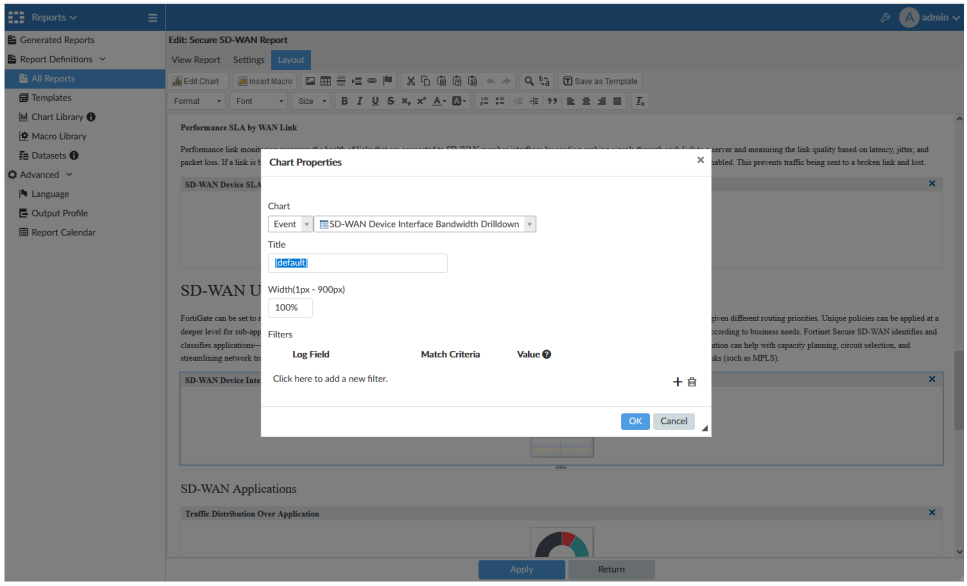
4. In the reports pane, expand *FortiGate Reports* and click *Secure SD-WAN Report*.



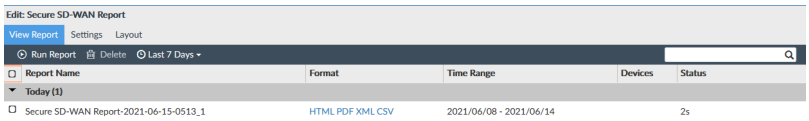
5. Click the *Layout* tab and scroll down to the *SD-WAN Link Health Status* chart, then click the *Chart Properties*. The *SD-WAN Device-Interface List by Activity* chart was added to the *Event* category.



6. Scroll down to the *SD-WAN Utilization* section and click the *Chart Properties*. The *SD-WAN Device Interface Bandwidth Drilldown* chart was added to the *Event* category.



7. Click the *View Report* tab. In the *Format* column, click *PDF*.



The Table of Contents displays the *SD-WAN Link Health Status* report.

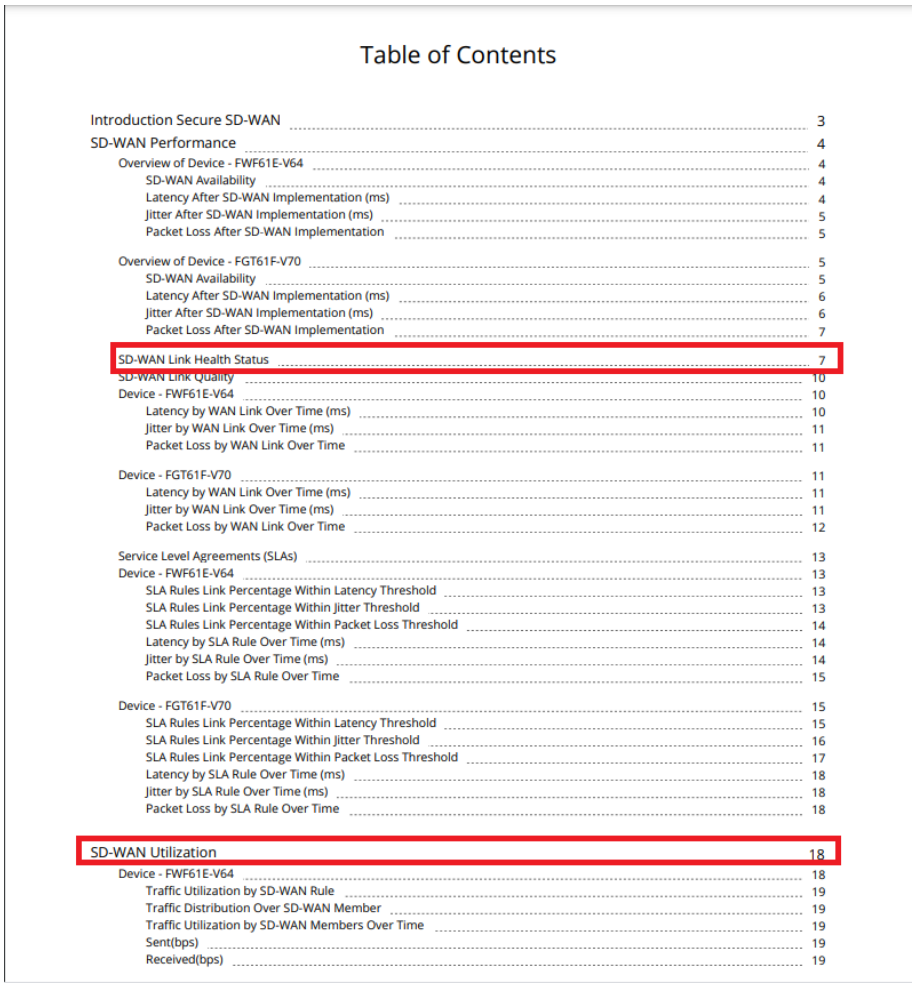
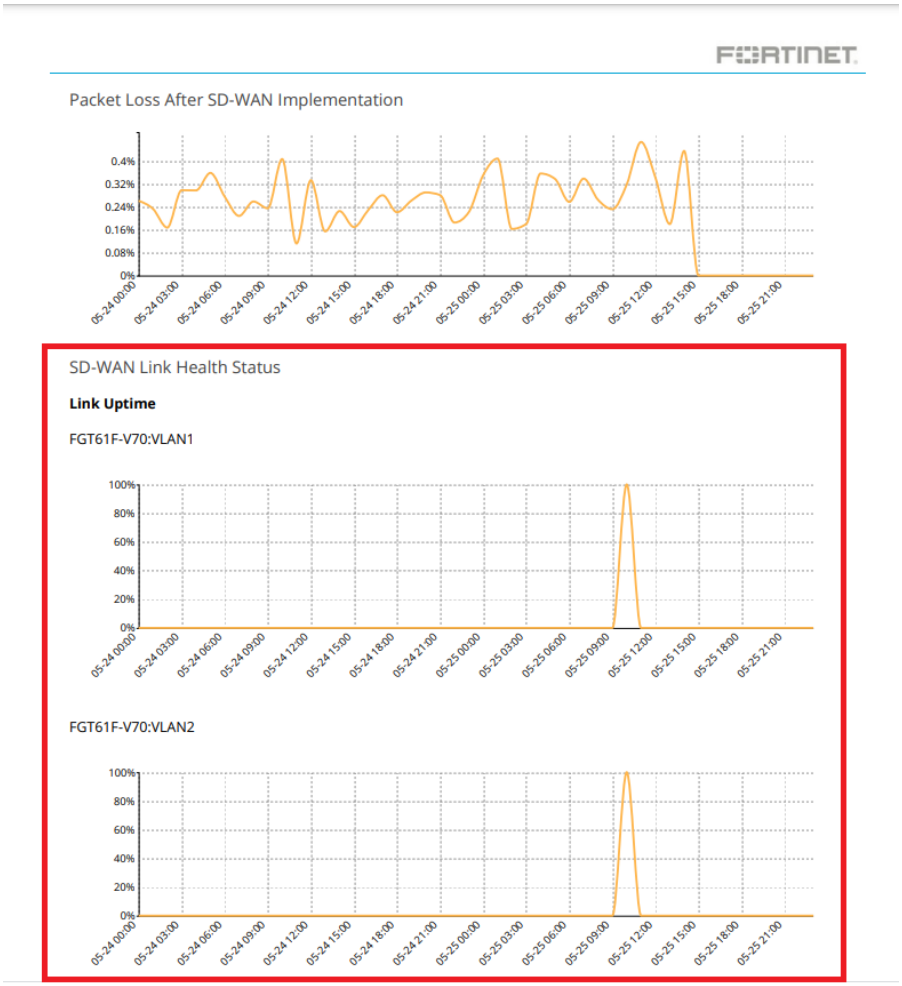
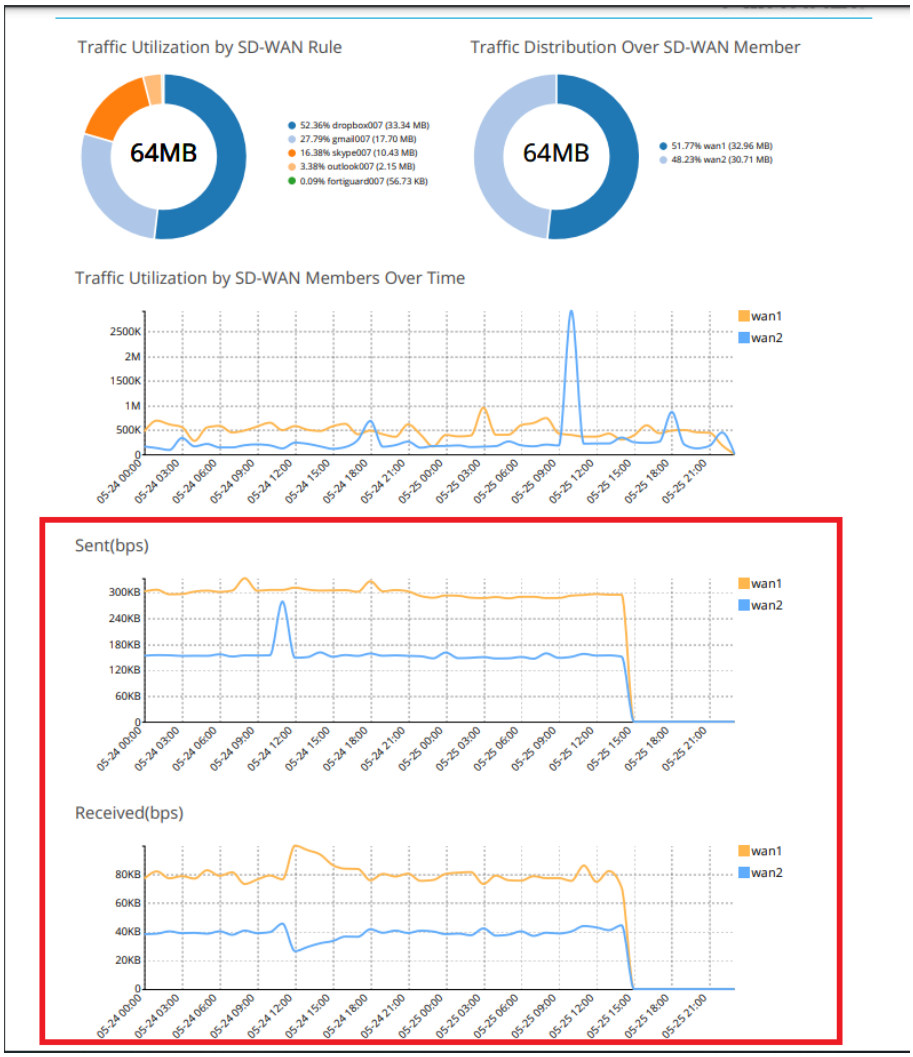


Table of Contents

The *SD-WAN Device-Interface List by Availability* drilldown charts are displayed.



The *SD-Wan Device Interface Bandwidth Drilldown* charts are also displayed.


Traffic Utilization by SD-WAN Rule
64MB
52.36% dropbox007 (33.34 MB)
27.79% gmail007 (17.70 MB)
16.38% skype007 (10.43 MB)
3.38% outlook007 (2.15 MB)
0.09% fortiguard007 (56.73 KB)
Traffic Distribution Over SD-WAN Member
64MB
51.77% wan1 (32.96 MB)
48.23% wan2 (30.71 MB)
Traffic Utilization by SD-WAN Members Over Time
wan1
wan2
2500K
2M
1500K
1M
500K
0
05-24 00:00
05-24 03:00
05-24 06:00
05-24 09:00
05-24 12:00
05-24 15:00
05-24 18:00
05-24 21:00
05-25 00:00
05-25 03:00
05-25 06:00
05-25 09:00
05-25 12:00
05-25 15:00
05-25 18:00
05-25 21:00
Sent(bps)
wan1
wan2
300KB
240KB
180KB
120KB
60KB
0
Received(bps)
wan1
wan2
80KB
60KB
40KB
20KB
0

System

This section lists the new features added to FortiAnalyzer for system settings:

High Availability (HA)

This section lists the new features added to FortiAnalyzer for high availability (HA):

FortiAnalyzer HA graceful upgrade

With this new feature, FortiAnalyzer HA supports graceful upgrading to avoid log loss, and also allow a trial period of the new image and support roll-back to the existing firmware if the new image has any issues.

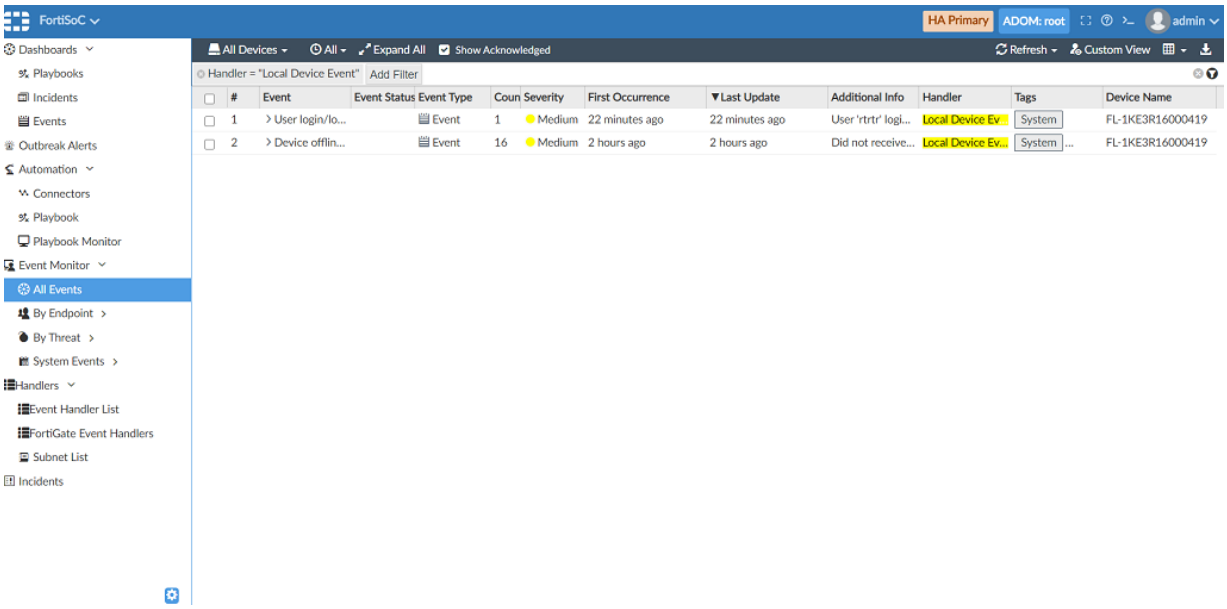
In the following example, FortiAnalyzer HA is being upgraded from version 6.4.5 to 7.0.0, and contains two members: *FAZ-1* is the Primary and *FAZ-2* is the Secondary.

Graceful upgrade is only supported when upgrading from 6.4.5 and above to version 7.0.0 and later.

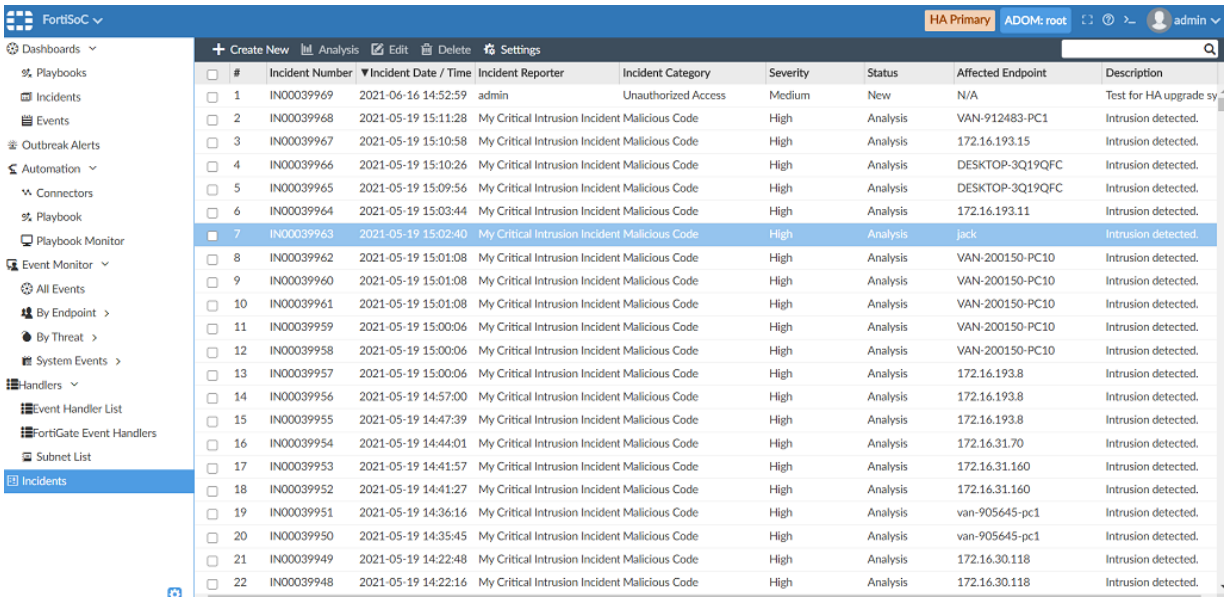
Data conversion depends on each application using this framework to do the conversion between the different versions. In 7.0.0, only incident conversion is supported when syncing from a higher level version to lower level version.

To update FortiAnalyzer HA gracefully:

1. Upgrade FAZ-2, the Secondary unit, to the new version. In this example, FAZ-2 is upgraded from version 6.4.5 to 7.0.0.
2. After FAZ-2 is up and running, check that there are no critical crashes and that the Primary can still forward logs to the Secondary. Event Alert and Incidents still can be received from 6.4.5 to 7.0.0.
   - To check that there are no critical crashes, use the following CLI command:
     ```
     diagnose debug crash read
     ```
   - To check that logs are being forwarded, use the following CLI command:
     ```
     diagnose test application logfwd 4
     ```
   - To create an example to check event alert synchronization, log in to FortiAnalyzer using the wrong password to generate a new local event log, and check on both FAZ-1 and FAZ-2 to confirm that the event alert can be found on both devices.



- To create an example to check incident synchronization, create a new incident on FAZ-1, then check on FAZ-2 to see if it was correctly synced across devices.



3. Since both devices are now running on different firmware versions, configuration synchronization is unavailable at this time. You can check this setting using the `diagnose ha status` command in the FortiAnalyzer CLI.
   In this example, the config sync status is down, and no configuration changes can be synced from the Primary to Secondary unit.

```
diagnose ha status
  HA-Status: Primary
  up-time: 11h38m12.811s
  config-sync: Allow
  serial-no: FL-1KE3R16000432
  fazuid: 2626920937
  hostname: FAZ1000E-2
  HA-Secondary HA1000e@192.168.1.90 FL-1KE3R16000419
  ip: 192.168.1.90
```

```
serial-no: FL-1KE3R16000119
fazuid: 1239922567
hostname: FAZ1000E
conn-st: up
up/down-time: 11h38m10.455s
conn-msg: firmware version mismatch (v6.4.6-build2363 210531 (GA))
cfgsync-st: down
data-init-sync-st: done, 11h37m49.396s
```

4. Once FAZ-2 is in data-sync with FAZ-1, an administrator can trigger HA-failover using the CLI to switch FAZ-2 to the Primary role.
   a. In the FortiAnalyzer CLI, enter the command `diagnose ha failover` to make FAZ-2 the Primary.
      ```
      FAZ1000E-1 # diagnose ha failover
      ```
   b. Use the command *diagnose ha status* to confirm the role of FAZ-2 as the new Primary.
      ```
      FAZ1000E-2 # diagnose ha status
         HA-Status: Primary
         up-time: 11h38m12.811s
         config-sync: Allow
         serial-no: FL-1KE3R16000432
         fazuid: 2626920937
         hostname: FAZ1000E-2
         HA-Secondary HA1000e@192.168.1.90 FL-1KE3R16000419
         ip: 192.168.1.90
         serial-no: FL-1KE3R16000119
         fazuid: 1239922567
         hostname: FAZ1000E
         conn-st: up
         up/down-time: 11h38m10.455s
         conn-msg: firmware version mismatch (v6.4.6-build2363 210531 (GA))
         cfgsync-st: down
         data-init-sync-st: done, 11h37m49.396s
      ```
5. Now is the time for the administrator to try out the new image on FAZ-2.
   As part of the graceful upgrade, logs can still be forwarded from a higher version (7.0.0) to a lower version (6.4.5) without issue, and incidents are synched from the higher version (7.0.0) to the Secondary running a lower version (6.4.5).
   During this time you should avoid any configuration changes, as they will not be synchronized between versions.
6. Check the upgrade guide checklist to confirm the new Primary is working as expected.
   After a few hours or a day, FAZ-1 can be upgraded to the new firmware version (7.0.0). After FAZ-1 is upgraded, FAZ-2 will continue to operate as the Primary. You can failover again to return FAZ-1 to operating as the Primary, or keep FAZ-2 as the new Primary.

Administrators

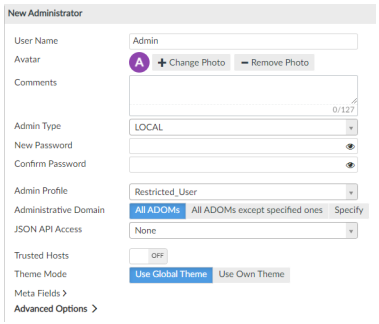
This section lists the new features added to FortiAnalyzer for administrators:

Theme mode

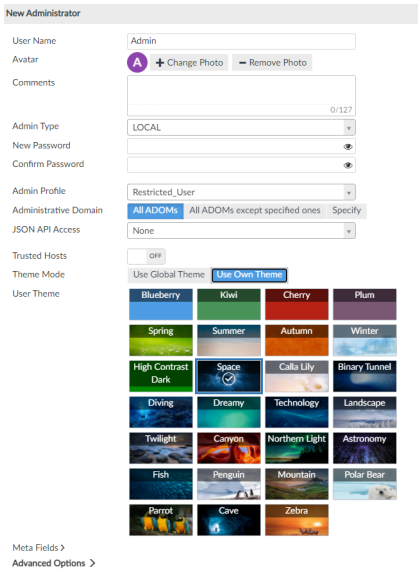
When you create a new user, you can to apply a theme to all the administrator accounts, or allow admins to choose their own theme

To enable themes per admin:

1. Go to *Admin* > *Administrators*.
2. In the toolbar, click *Create New*. The *New Administrator* page is displayed.

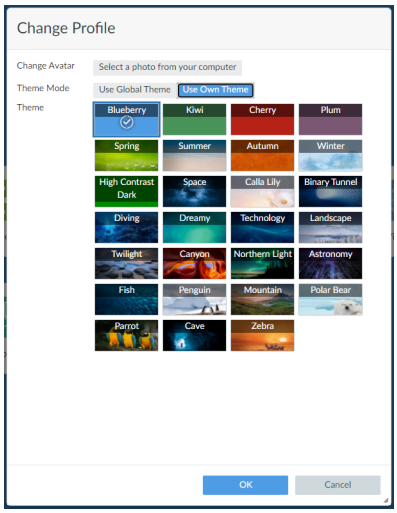


3. Set *Theme Mode* to *Use Own Theme*.
4. From the *User Theme* menu, select a theme.



5. Click *OK*.

When a user logs into their account, they can change the theme by clicking their username, and selecting *Change Profile*.

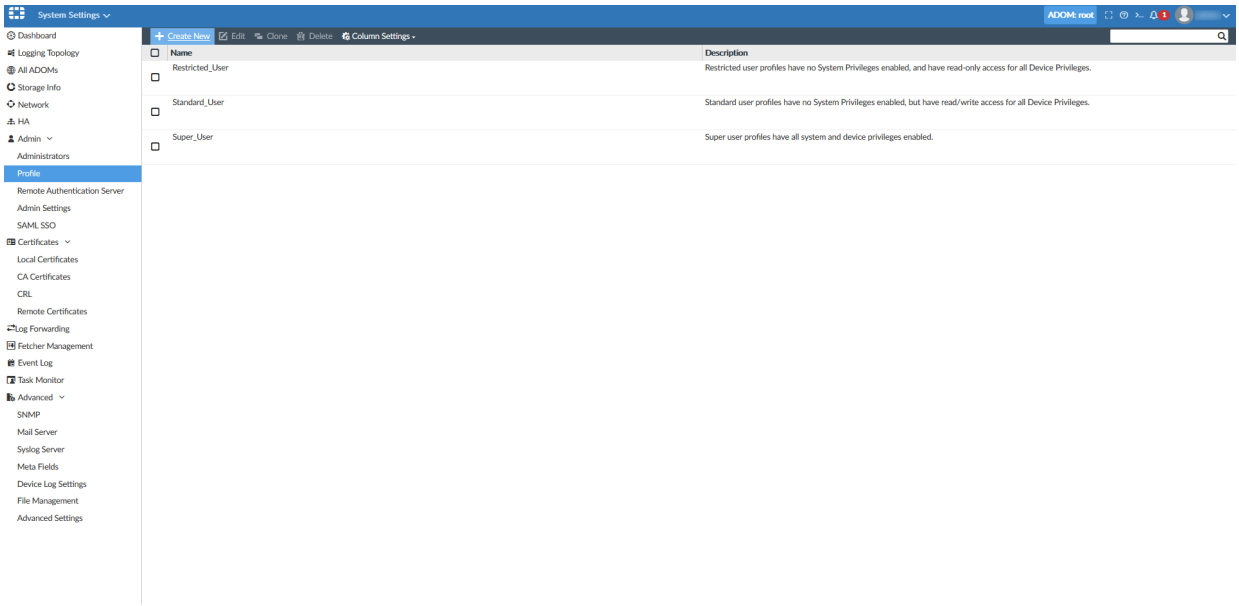


Add operation permissions to Admin profile

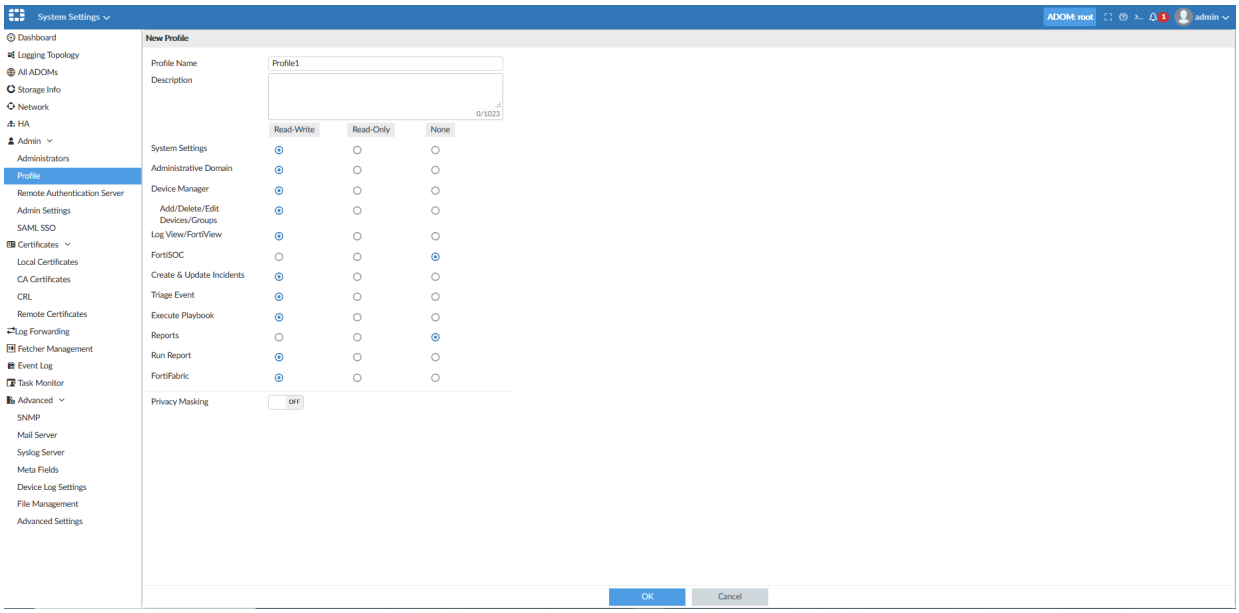
FortiSoC profile permissions grant administrators access to the FortiSoC module, while preventing them from making changes to the configuration that could affect the SLA.

To create a FortiSoC Admin profile:

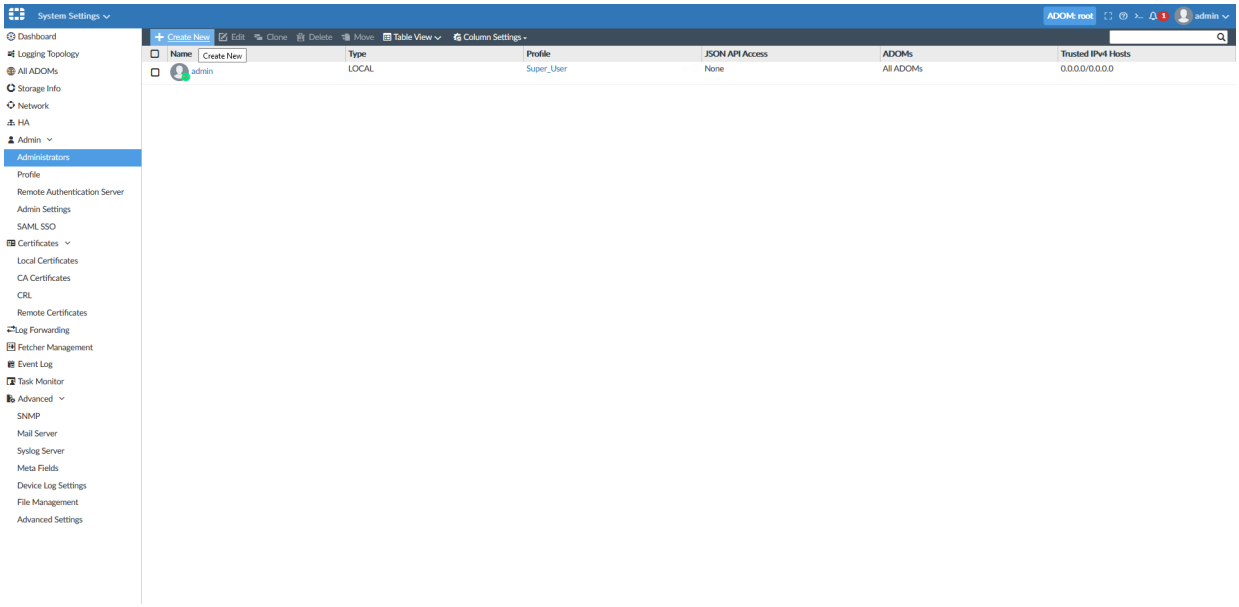
1. Go to *System Settings* > *Admin* > *Profile* > *Create New*.



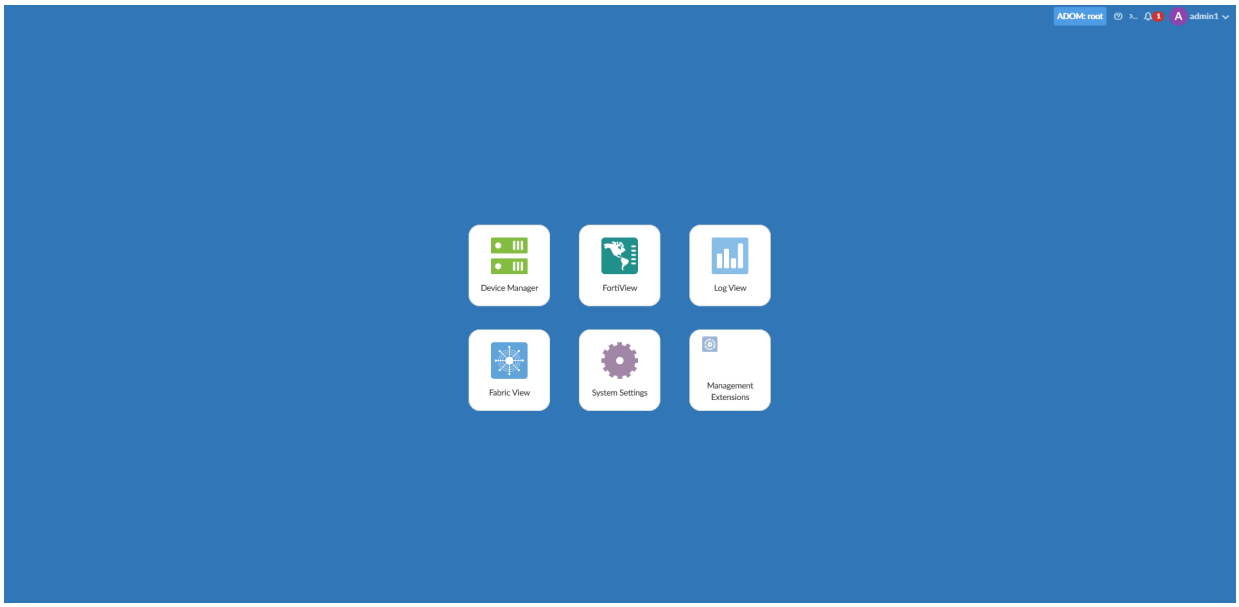
2. Configure the FortiSoC profile.
   a. Name the profile, *Profile1*.
   b. Set *FortSOC* to *None*.
   c. Set *Create & Update Incidents*, *Triage Event*, *Execute Playbook*, and *Run Report* to *Read-Write*.
   d. Click *OK*.



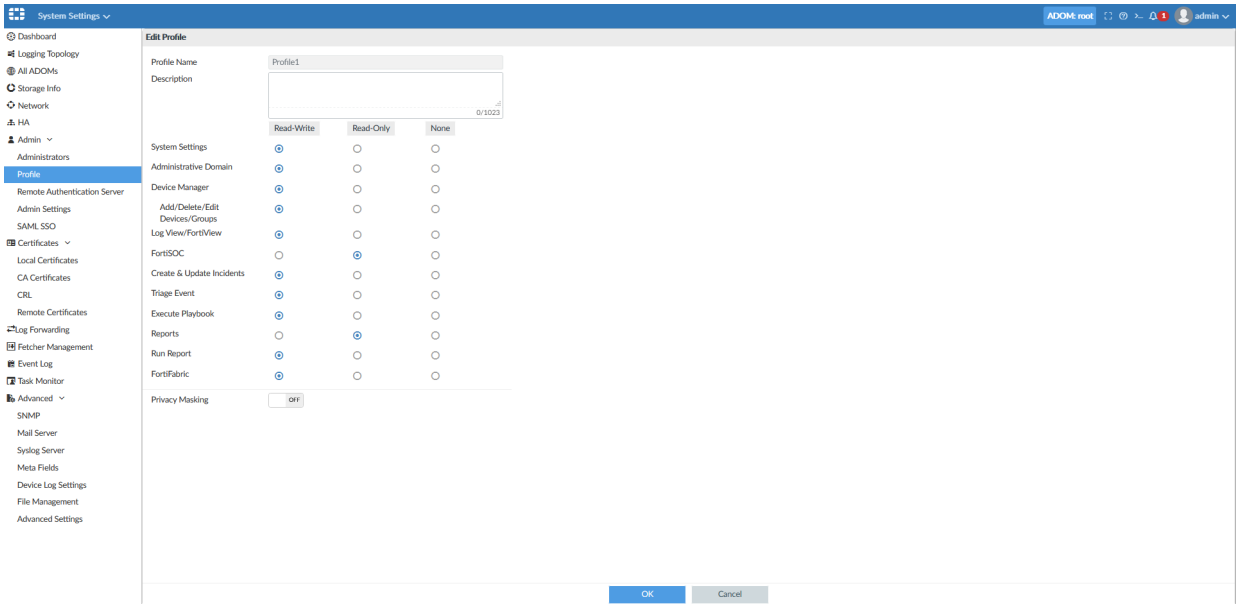
3. Apply the profile to an administrator account.
   a. Go to *System Settings* > *Admin* > *Administrators* > *Create New*.
   b. Name the new profile *Admin1*, and then select *Profile1* from the *Admin Profile* dropdown.
   c. Click *OK*.



4. Log out of FortiAnalyzer and then log back in as *Admin1*. The FortiSoC module is not available. Log out of the account.

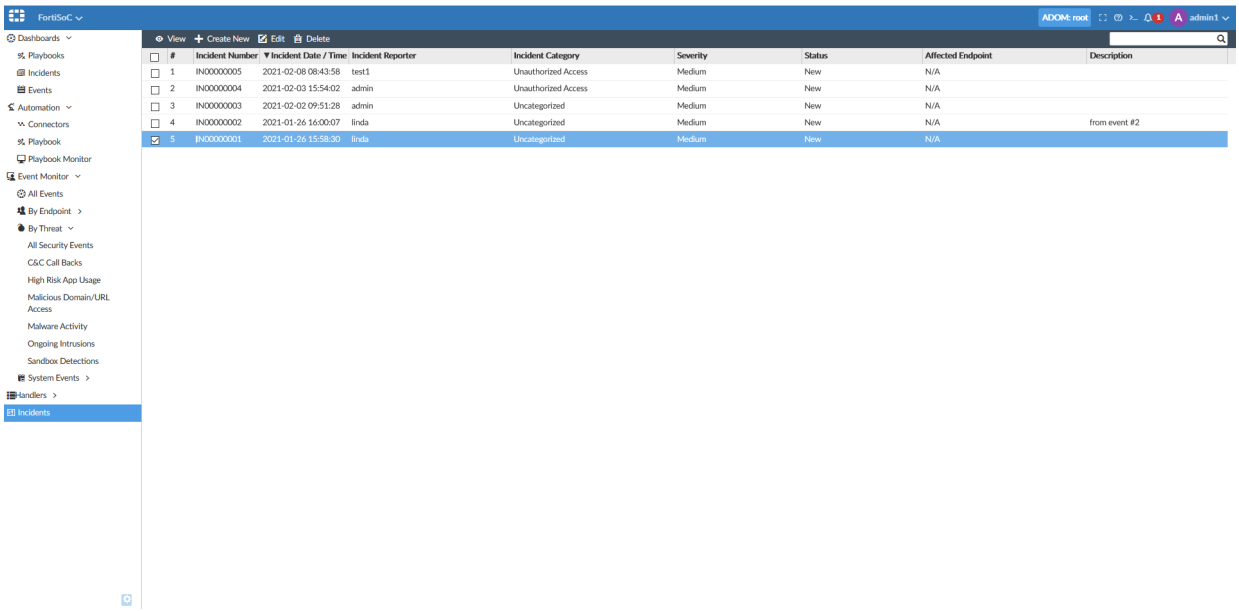


5. Log into FortiAnalyzer as an administrator, and go to *System Settings* > *Admin* > *Profile*.
6. Edit *Profile1*.
7. Set *FortiSOC* to *Read-Only*, and then click *OK*.

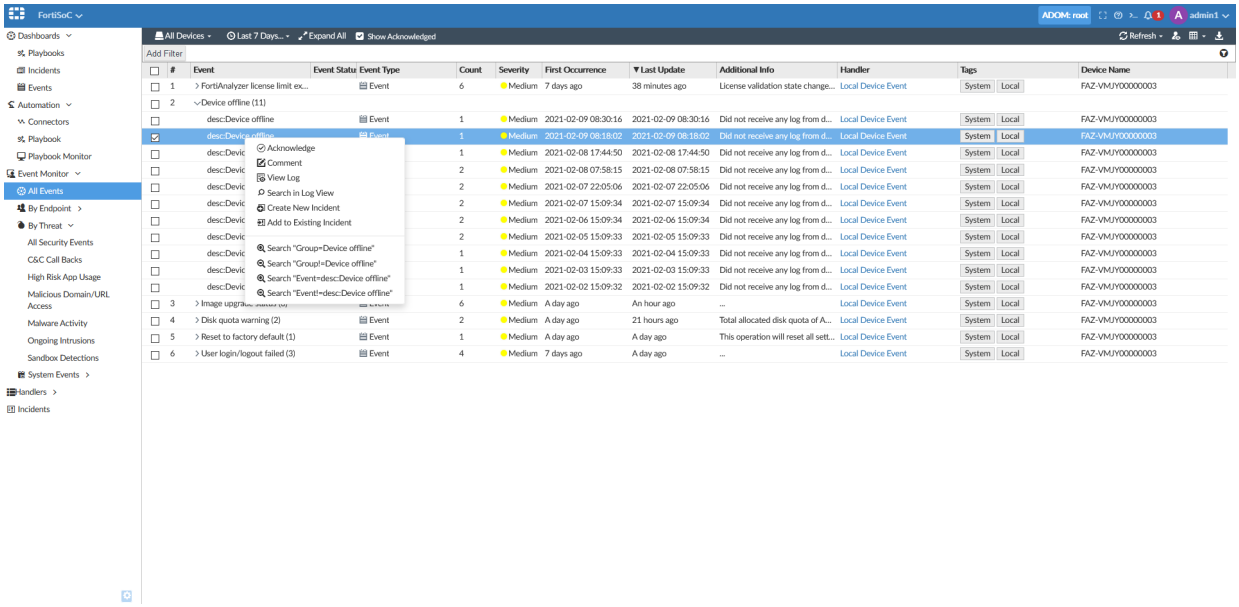


8. Log out of FortiAnalyzer, and then log back in as *Admin1*.

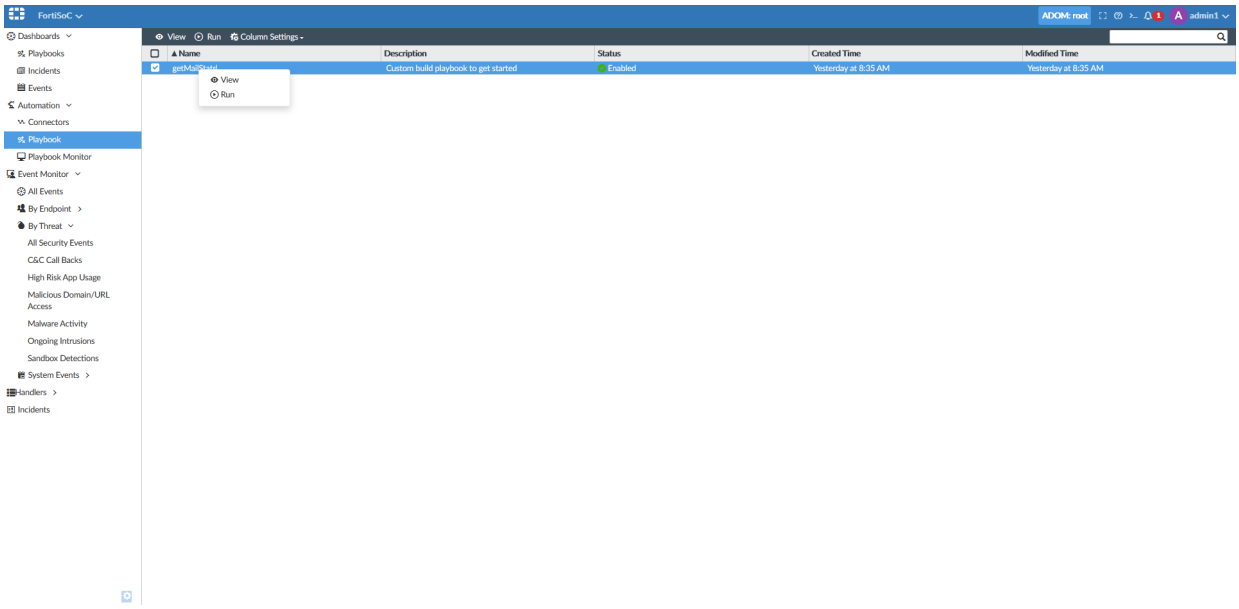
9. Go to *FortiSoC* > *Incidents*. You can view and create incidents.



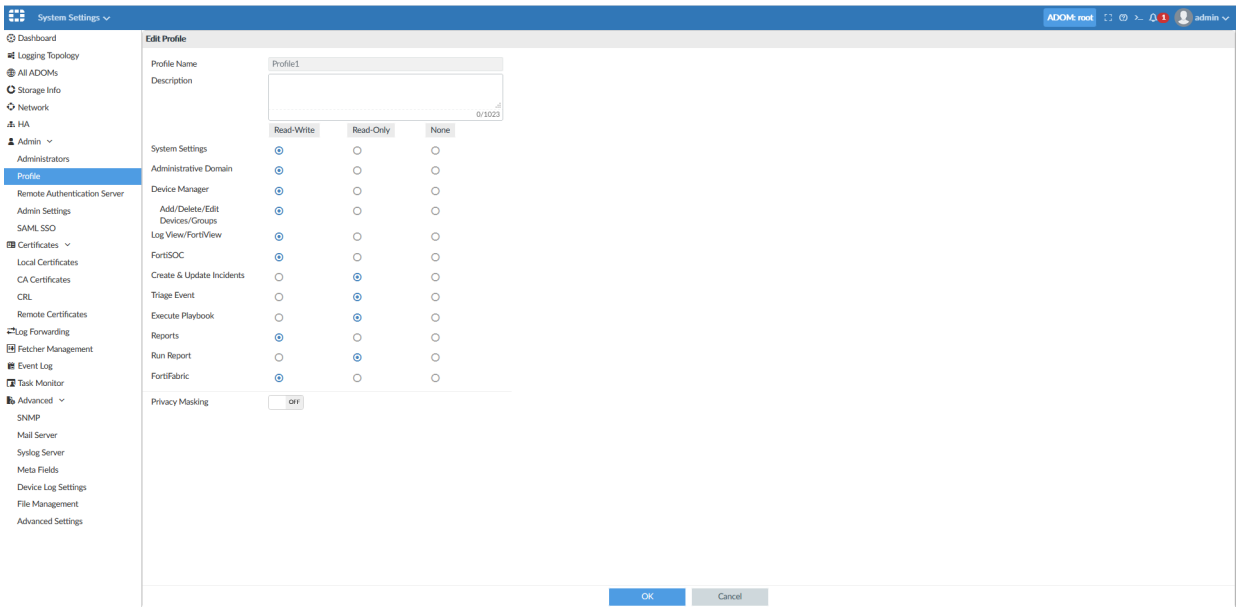
10. Go to *FortiSoC* > *All Events*. You can acknowledge, comment on, and create a new incident.



11. Go to *FortiSoC* > *Playbook*. You can now view and run a playbook.



12. Go to *Reports* > *All Reports*. You can view, run, and export FortiSoC reports.



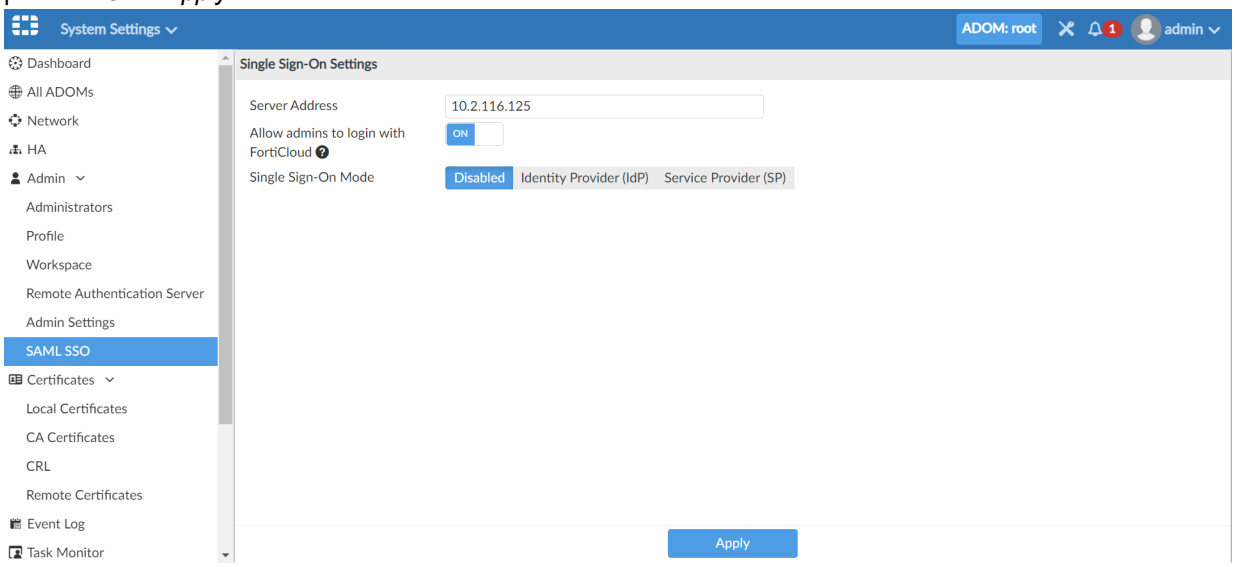
Admins can use a SAML SSO FortiCloud account to log in to FortiAnalyzer

Admins can use SAML SSO through their FortiCloud account to log in to FortiAnalyzer.

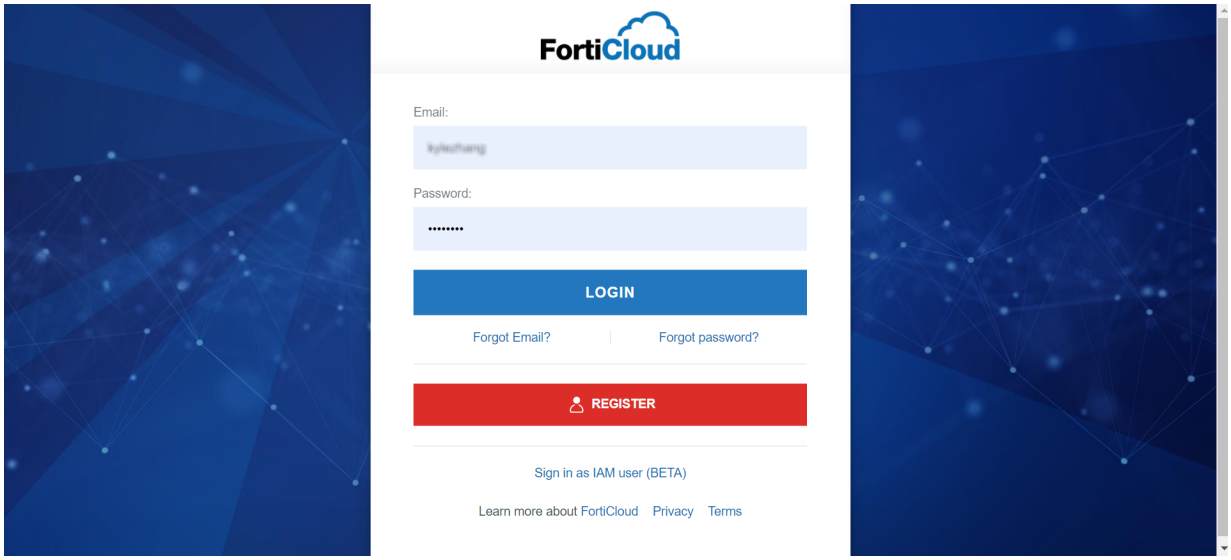
To enable SAML SSO using FortiCloud:

1. By default, administrators can only log in using a local or remote user account configured on FortiAnalyzer.
2. To enable SAML SSO using FortiCloud, you must first register your FortiAnalyzer on FortiCloud. You can confirm the FortiCloud registration status in *System Settings* > *Dashboard* under *License Information*.

3. Go to *System Settings* > *Admin* > *SAML SSO*, and set the *Allow admins to login with FortiCloud* toggle to the *ON* position. Click *Apply*.



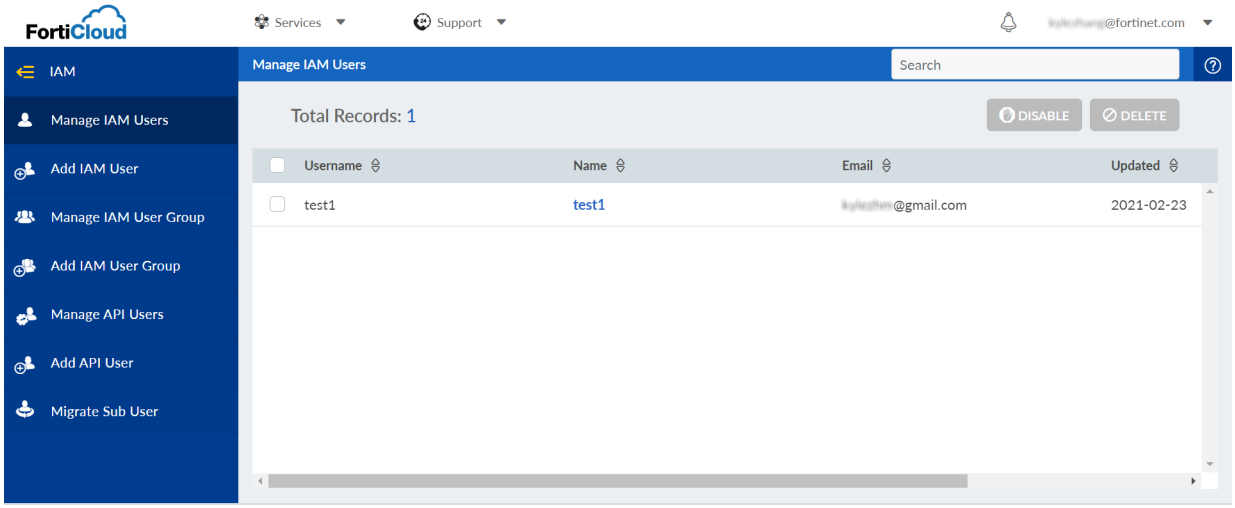
4. Sign out of FortiAnalyzer and return to the login page.
   You can now see a new option to log in using your FortiCloud account.
5. Click *Login with FortiCloud* and you are redirected to the FortiCloud login portal. Enter your FortiCloud credentials, and click *LOGIN*.



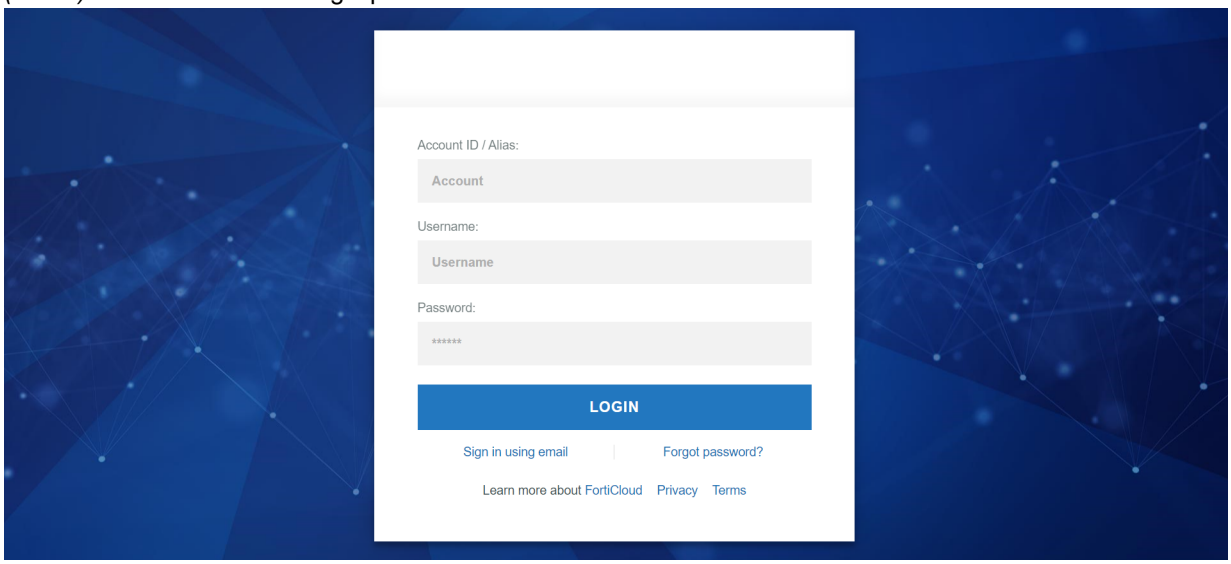
You are logged in to FortiAnalyzer with your FortiCloud account.

By default, only the account ID which the FortiAnalyzer is registered to can be used to log in to FortiAnalyzer. To enable login for additional user accounts using FortiCloud, you can configure multiple IAM users in FortiCloud.

6. Go to FortiCloud and create one or more IAM users. For more information on creating an IAM user, see Identity & Access Management (IAM).



7. Go to the FortiAnalyzer sign in page and click *Login with FortiCloud*, and click the option to *Sign in as IAM user (BETA)* at the bottom of the login portal.



8. Enter your IAM user credentials, and you will be logged in to FortiAnalyzer as the IAM user.

ADOM

This section lists the new features added to FortiAnalyzer for ADOMs:

- Support for link aggregation on page 92

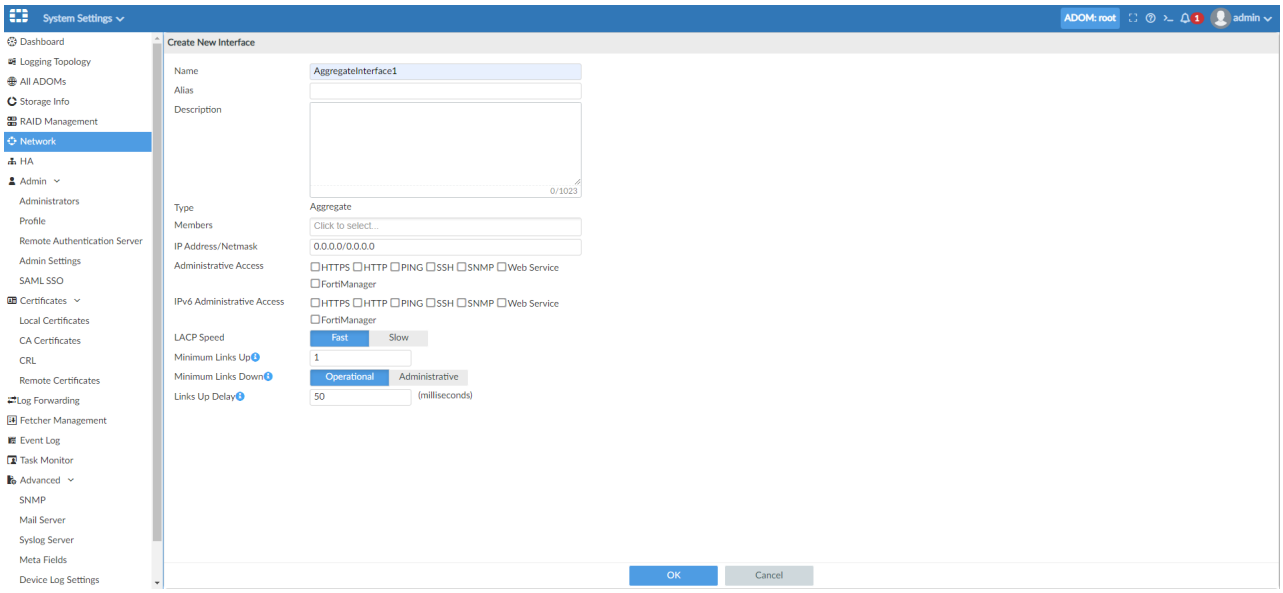
Support for link aggregation

Interface link-aggregation is now supported on high-end FortiAnalyzer appliances and VM platforms to provide interface redundancy and load balance.

This feature is only available in high-end FortiAnalyzer devices (FAZ2000E and above), and VM platforms.

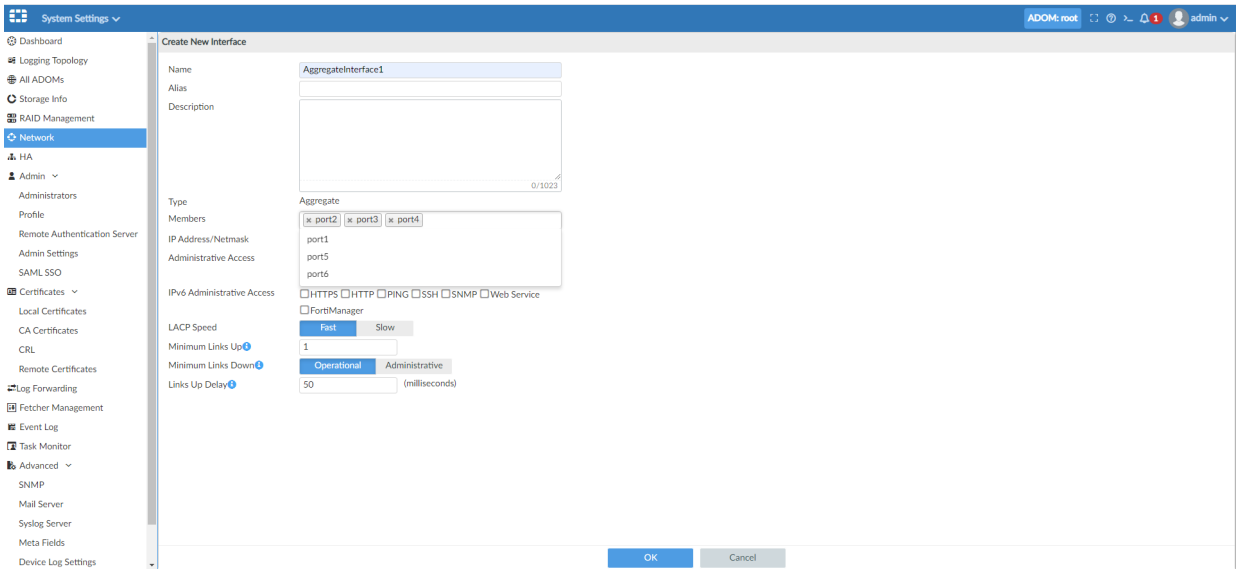
To create an aggregate interface in the GUI:

1. Go to *System Settings* > *Network*.
2. In the toolbar, click *Create New*. The *Create New Interface* window opens.

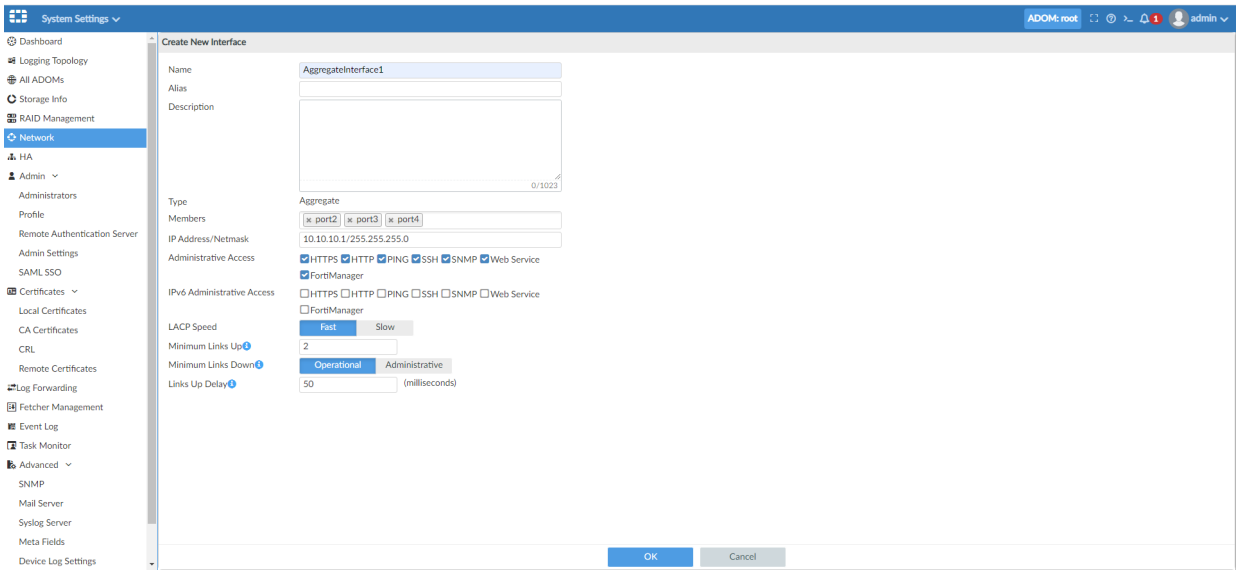


3. In the *Name* field, enter a name for the interface (for example, `Aggregation1`)

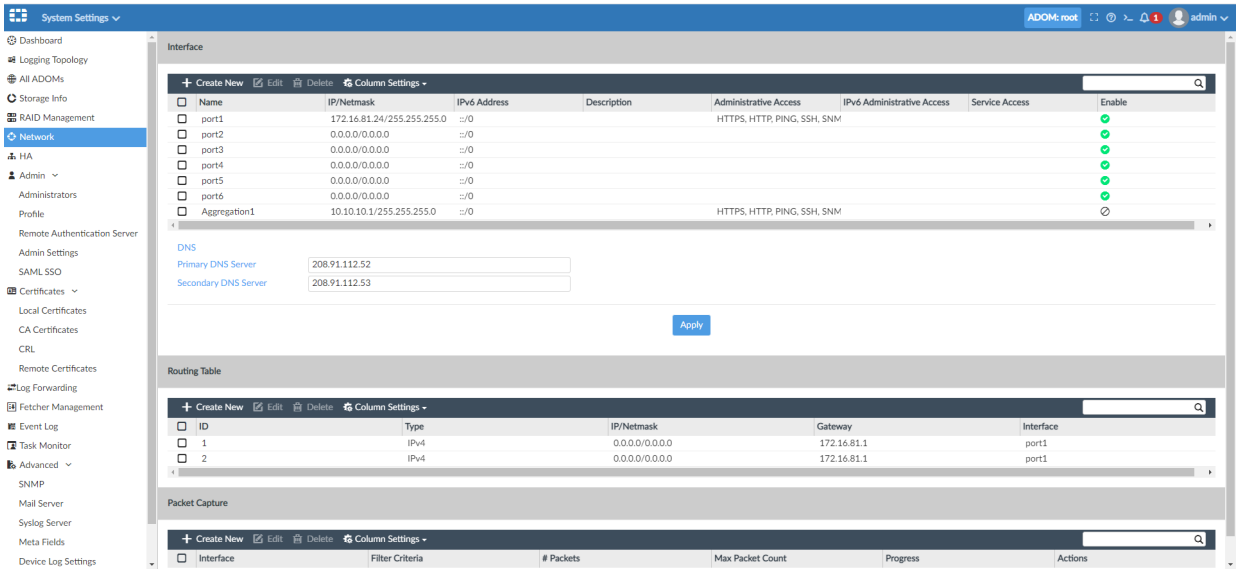
4. Click the *Members* field to select the available ports.



5. In the *IP Address/Netmask* field, enter a minimum of two IP addresses. At least two ports need to be up for the aggregate interface to work.



6. Apply the default settings for the rest of the configurations.



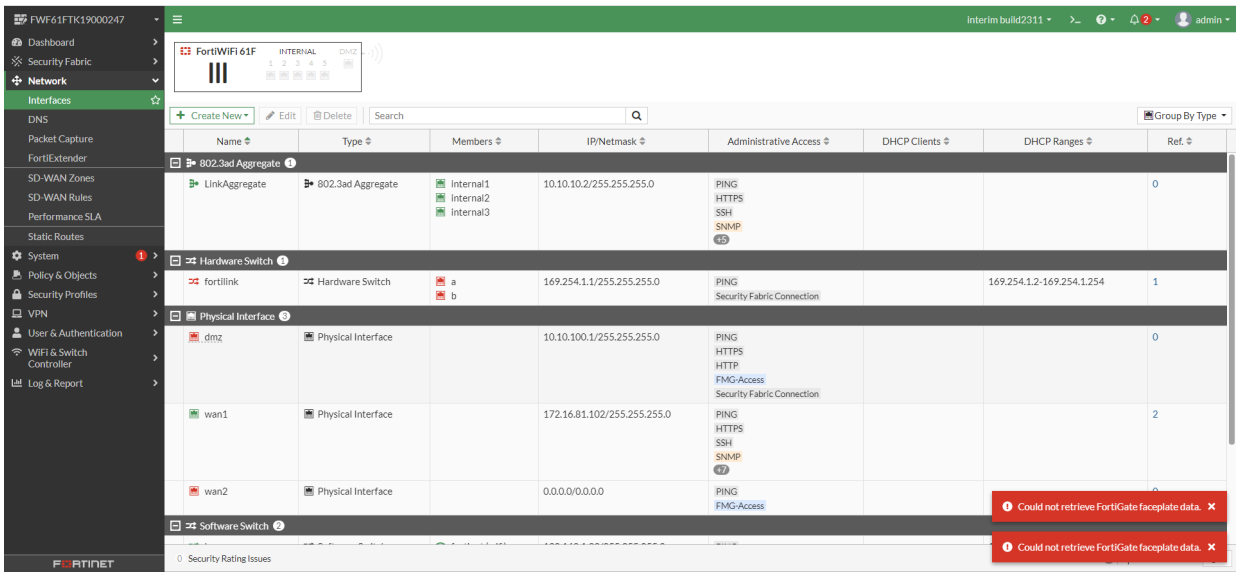
7. Click *OK*. The aggregation interface is created.

To verify the aggregate interface is up with the CLI:

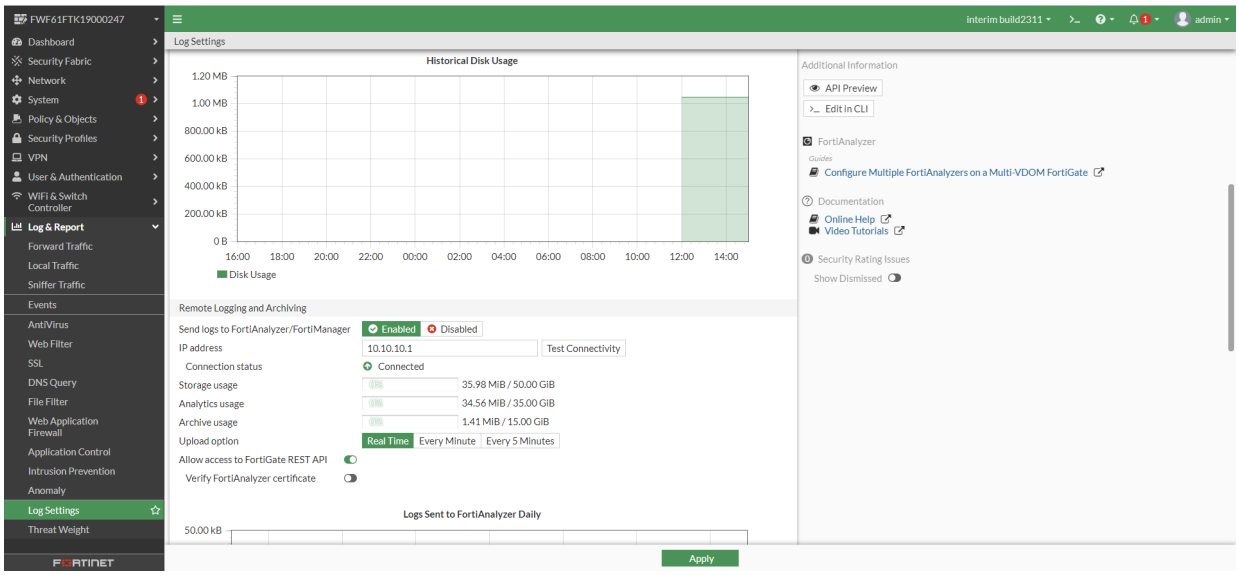
```
FAZ3000F # config system interface
(interface)# edit Aggregation1
(Aggregation1)# set status up
(Aggregation1)# end
FAZ3000F #
```

To configure the aggregation interface in FortiGate:

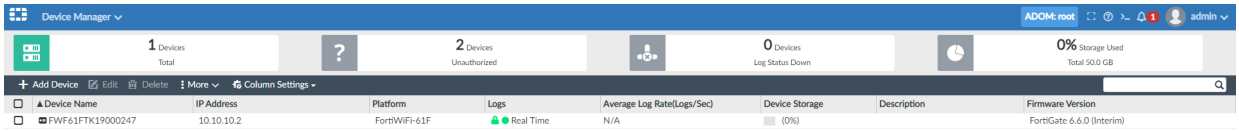
1. In FortiGate go to *Network* > *Interfaces*, and configure the aggregation interface using the same subnet as FortiAnalyzer.



2. Go to *Log & Report* > *Log Settings*, and configure the logs sent to FortiAnalyzer through the aggregation interface.



3. In FortiAnalyzer, go to *Device Manager* to confirm FortiGate has established a connection with FortiAnalyzer through the aggregation interface.



Management Extensions

This section lists the other new features added to FortiAnalyzer for management extensions:

New management extension - FortiSOAR

This feature adds the FortiSOAR application as a management extension application (MEA). FortiSOAR is an enterprise-built security orchestration and security automation workbench that empowers security operation teams.

By default, FortiSOAR MEA is disabled. You can enable FortiSOAR MEA by using the GUI or the CLI.

There are minimum system resources recommended for FortiAnalyzer when using FortiSOAR MEA. See the FortiAnalyzer Release Notes for additional information.

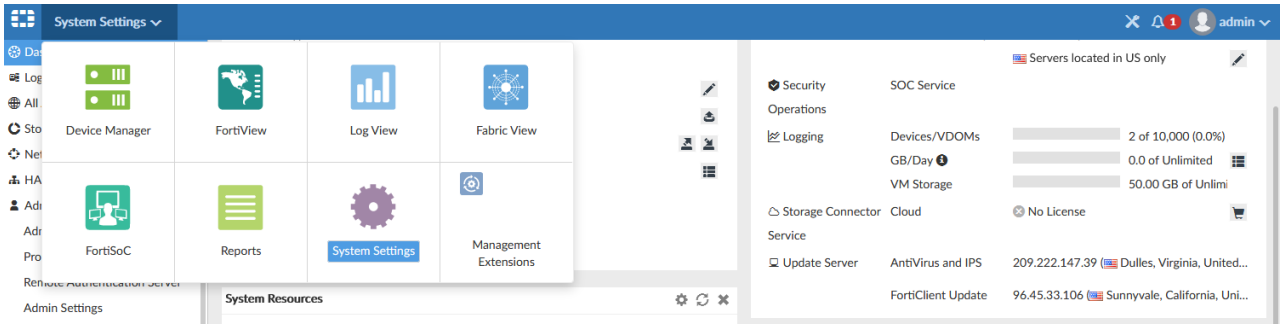
The following CLI commands are available for FortiSOAR MEA:

- `config system docker`
- `diagnose docker status`
- `diagnose docker upgrade fortisoar`

FortiAnalyzer supports only FortiSOAR MEA. Although you can use the CLI to enable additional management extension applications, they are not supported by FortiAnalyzer. Enabled, unsupported management extension applications are hidden from the FortiAnalyzer GUI, but still consume valuable resources. Be sure to only enable FortiSOAR MEA on FortiAnalyzer when using the CLI.

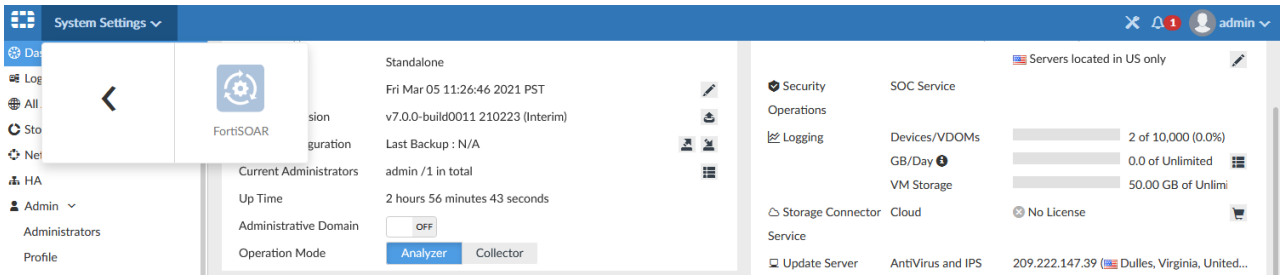
To enable FortiSOAR MEA by using the GUI:

1. Go to the *Management Extensions* tile.



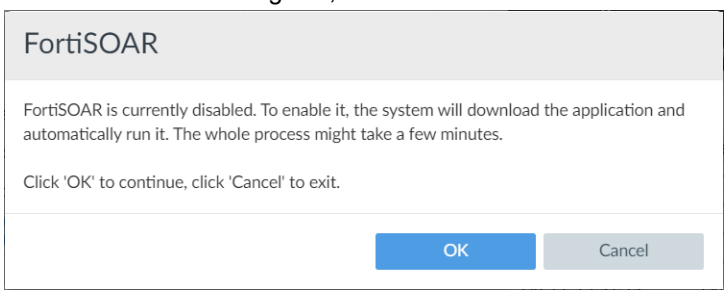
The management extension application options are displayed.

2. Click *FortiSOAR*.



A confirmation dialog box is displayed.

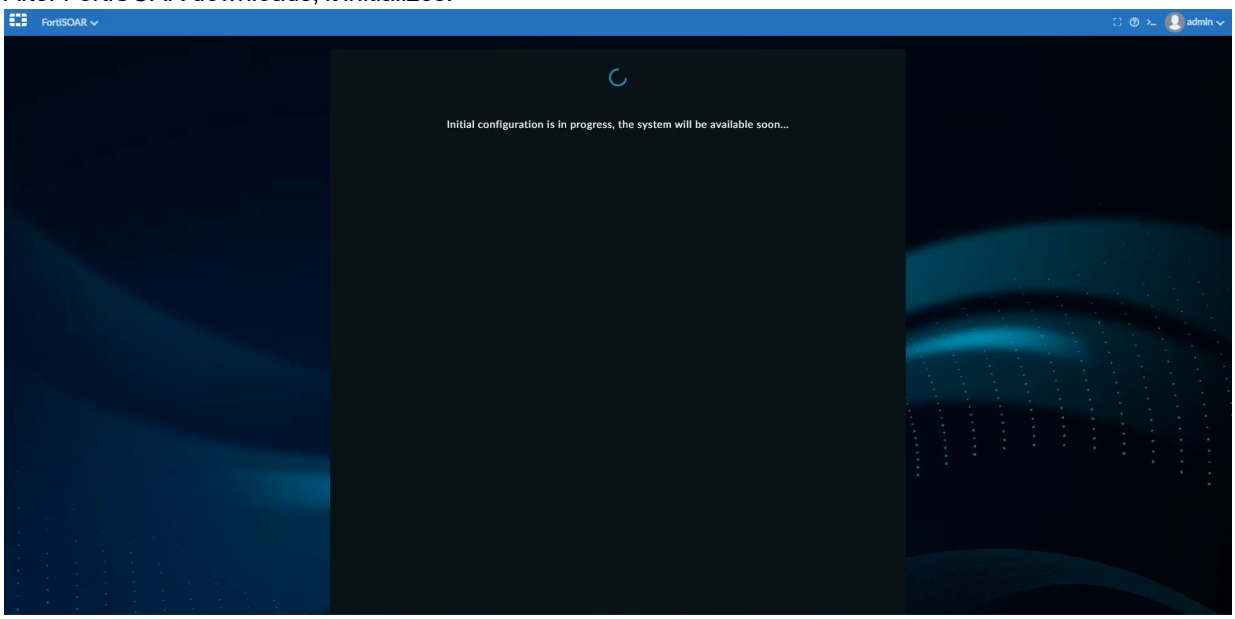
3. In the confirmation dialog box, click *OK*.



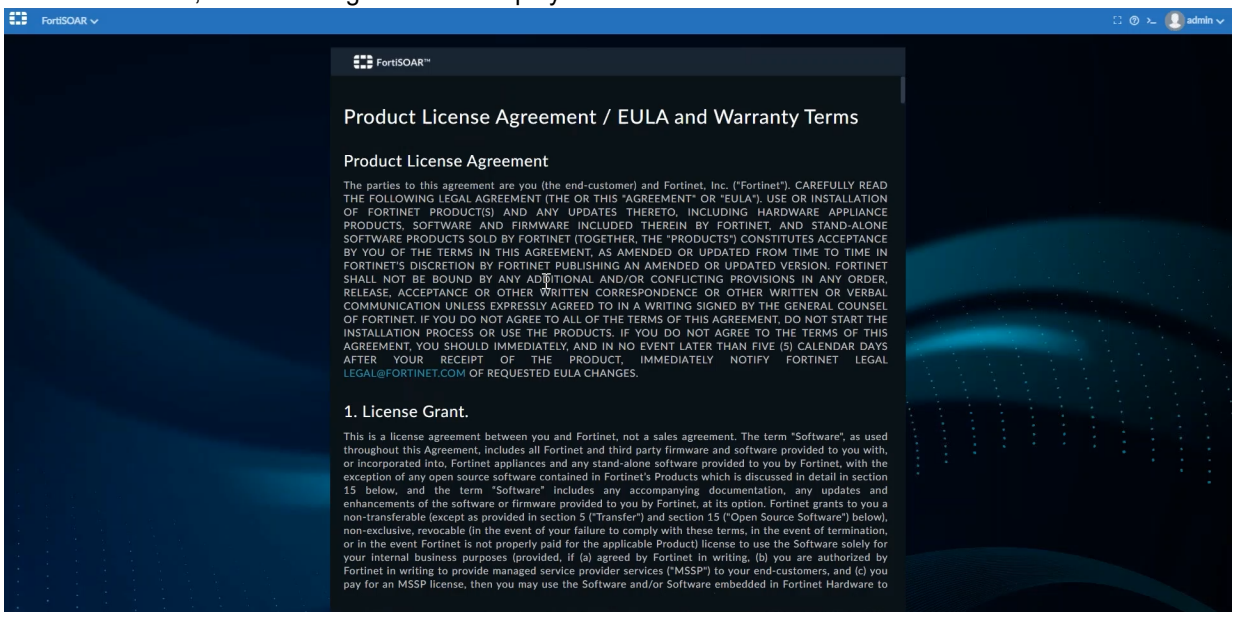
FortiSOAR MEA is downloaded from the Fortinet registry (registry.fortinet.com).

A progress bar displays under the FortiSOAR tile.

After FortiSOAR downloads, it initializes.

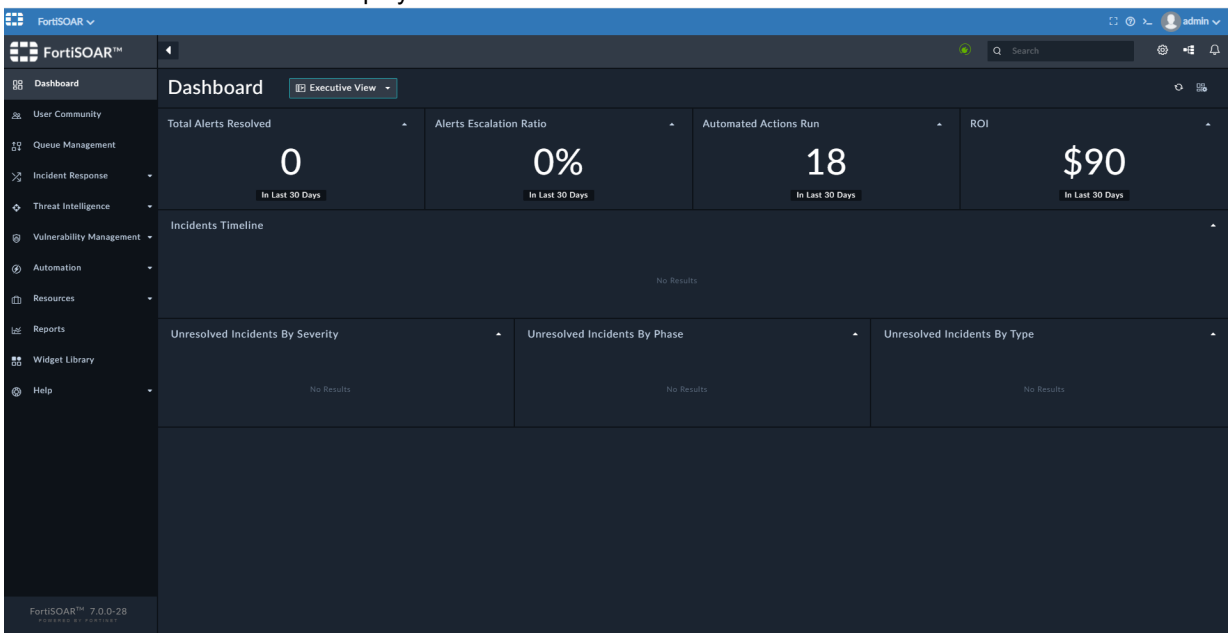


After initialization, the license agreement is displayed.

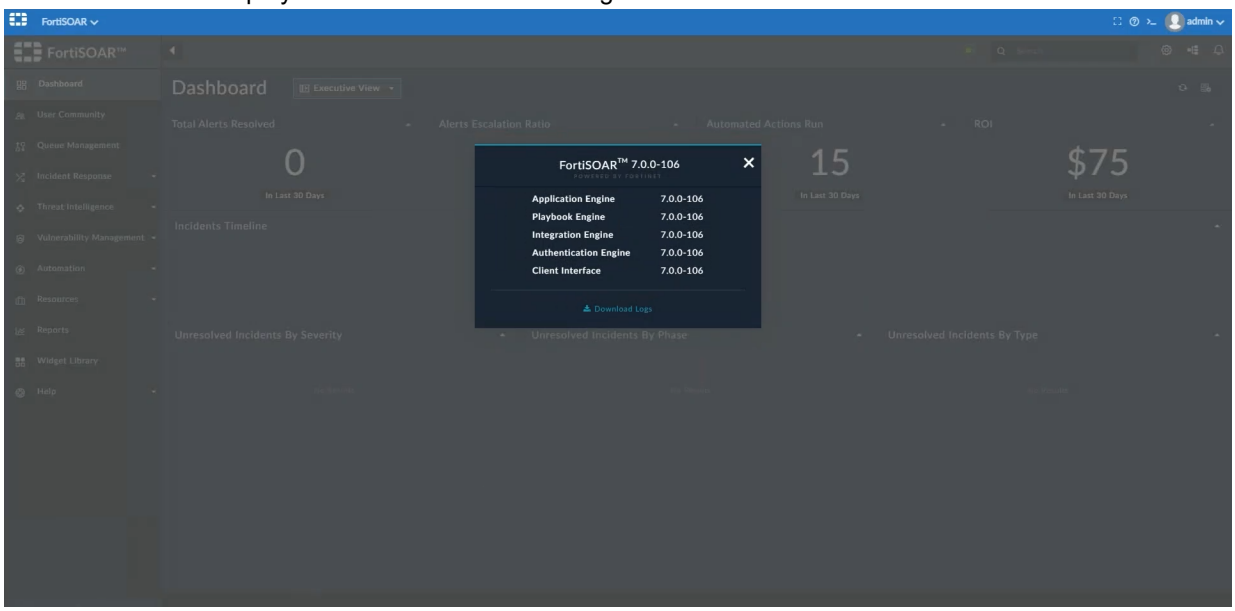


4. Read the license agreement, and click *Agree*.

5. Log in to FortiSOAR by using your FortiAnalyzer login.
   The FortiSOAR dashboard is displayed.



The version and build information for FortiSOAR can be found on the bottom-left corner of the Dashboard. Clicking on this information displays the version and build dialog.



Other

This section lists the other new features added to FortiAnalyzer:

FortiAnalyzer Setup wizard

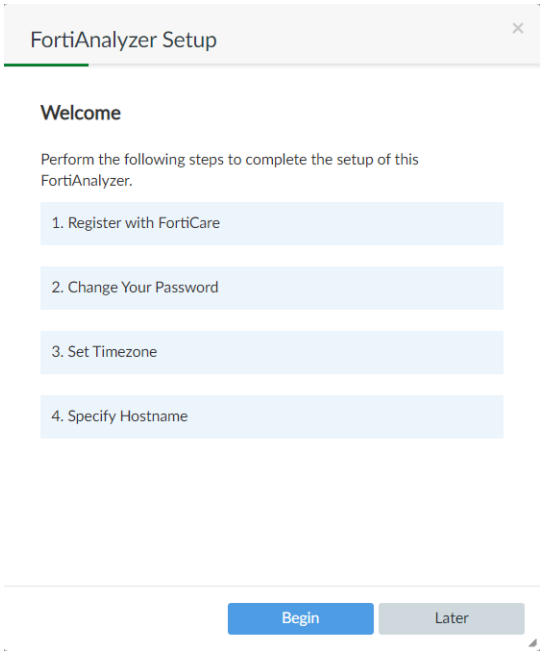
The FortiAnalyzer Setup wizard lets you register with FortiCare as well as perform the following actions:

- Registering with FortiCare
- Changing your password
- Setting the time zone
- Specifying a hostname

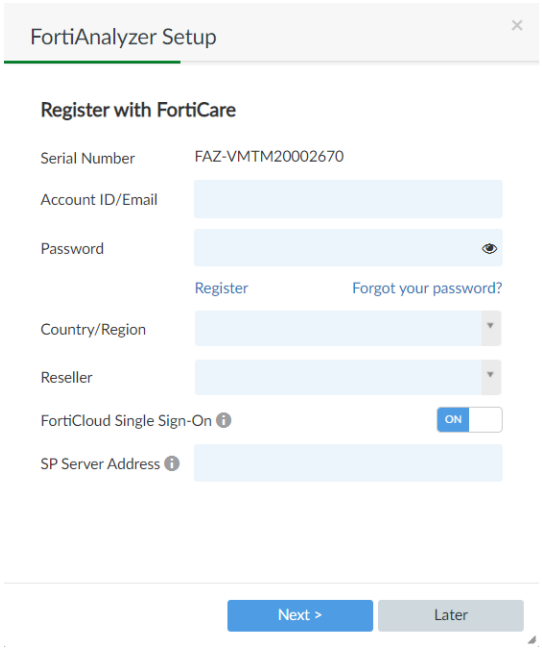
When an action is complete, a green checkmark displays it in the wizard, and the wizard no longer displays after you log in to FortiAnalyzer.

To use the FortiAnalyzer Setup wizard:

1. Log in to FortiAnalyzer.
   The *FortiAnalyzer Setup* dialog box is displayed.

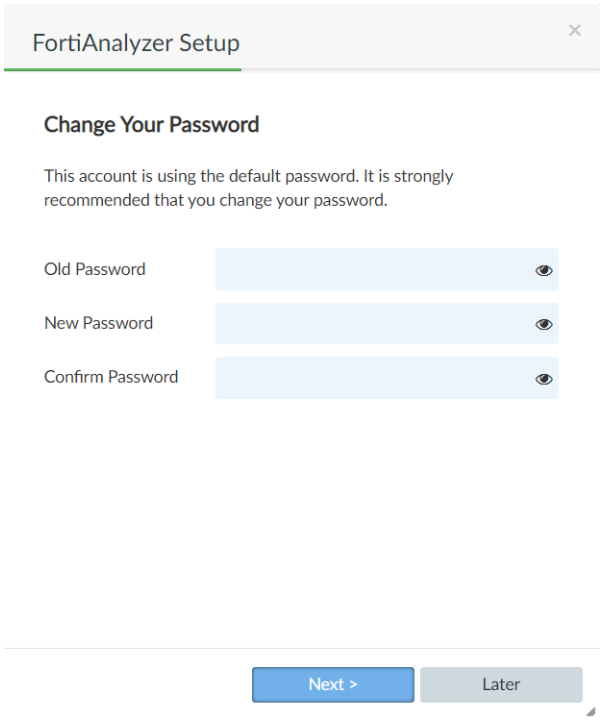


2. Click *Begin* to start the setup process now.
   Alternately, click *Later* to postpone the setup tasks.
3. When prompted, register with FortiCare.



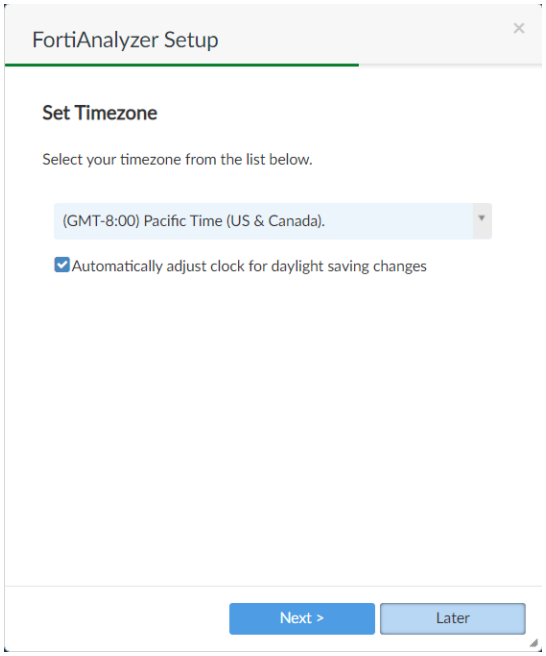
   a. In the *Account ID/Email* box, type your FortiCare account ID or email.
      If you do not yet have a FortiCare account, click *Register* to create a new account.
   b. In the *Password* box, type your FortiCare password.
      If you have forgotten your FortiCare password, click *Forgot your password* to proceed through the password recovery process.
   c. In the *Country/Region* box, select your country or region from the dropdown.
   d. In the *Reseller* box, select your reseller from the dropdown.
   e. Set the *FortiCloud Single Sign-On* toggle to the *ON* or *OFF* position to enable or disable FortiCloud SSO sign on.
      When enabled, you must also enter the *SP Server Address*.
   f. Click *Next*.

4. When prompted, change your password.



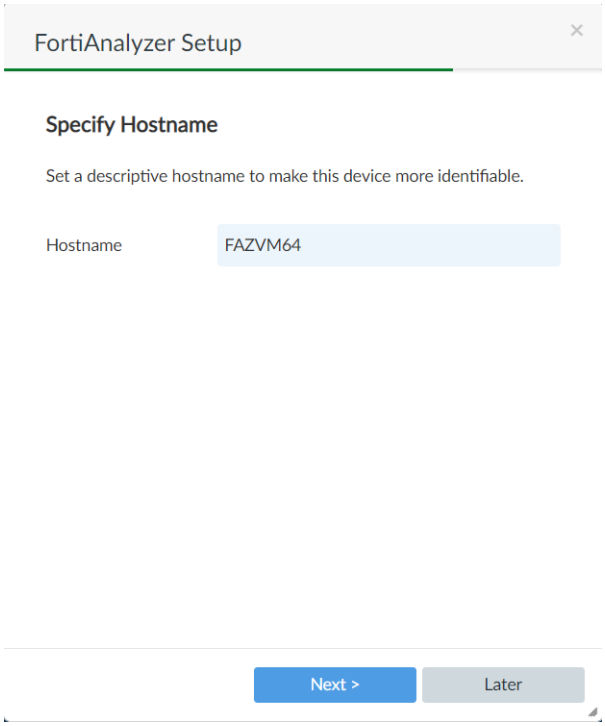
   a. In the *Old Password* box, type the old password.
   b. In the *New Password* box, type the new password.
   c. In the *Confirm Password* box, type the new password again.
   d. Click *Next*.

5. When prompted, set the time zone.



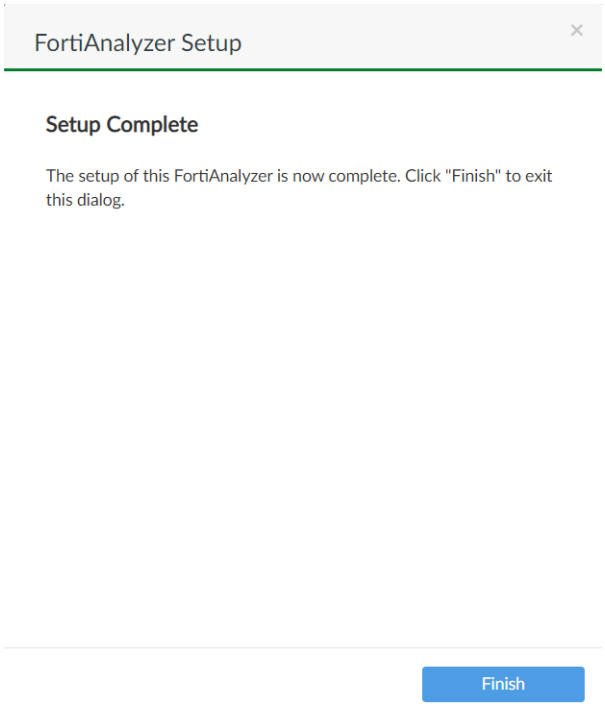
a. From the list, select the time zone.
b. (Optional) Clear the *Automatically adjust clock for daylight savings changes* checkbox if desired. By default FortiAnalyzer is configured to automatically adjust closed for daylight savings.
c. Click *Next*.

6. When prompted, specify the hostname.



a. In the *Hostname* box, type a hostname.
b. Click *Next*.

7. When prompted, complete the setup by clicking *Finish*.



You are logged in to FortiAnalyzer.

FortiAnalyzer VM licenses

For FortiAnalyzer virtual machines (VMs), you can use the FortiAnalyzer GUI to:

- Request and activate a trial license
- Activate a perpetual or VM-S license
- Activate an add-on perpetual or VM-S license

FortiAnalyzer must be able to access the Internet to communicate with FortiCloud to complete the licensing process.

The licensing process requires you to log in to FortiCloud. If you do not have a FortiCloud account, you can create one to complete the licensing process.

This topic contains the following sections:

- Requesting and activating a trial license on page 104
- Activating a new license on page 107
- Activating an add-on license on page 108

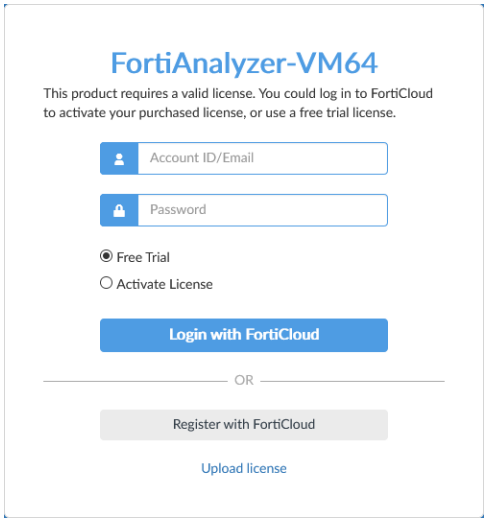
Some of the screen shots in the following examples are for FortiManager, but the process applies to both FortiManager and FortiAnalyzer.

Requesting and activating a trial license

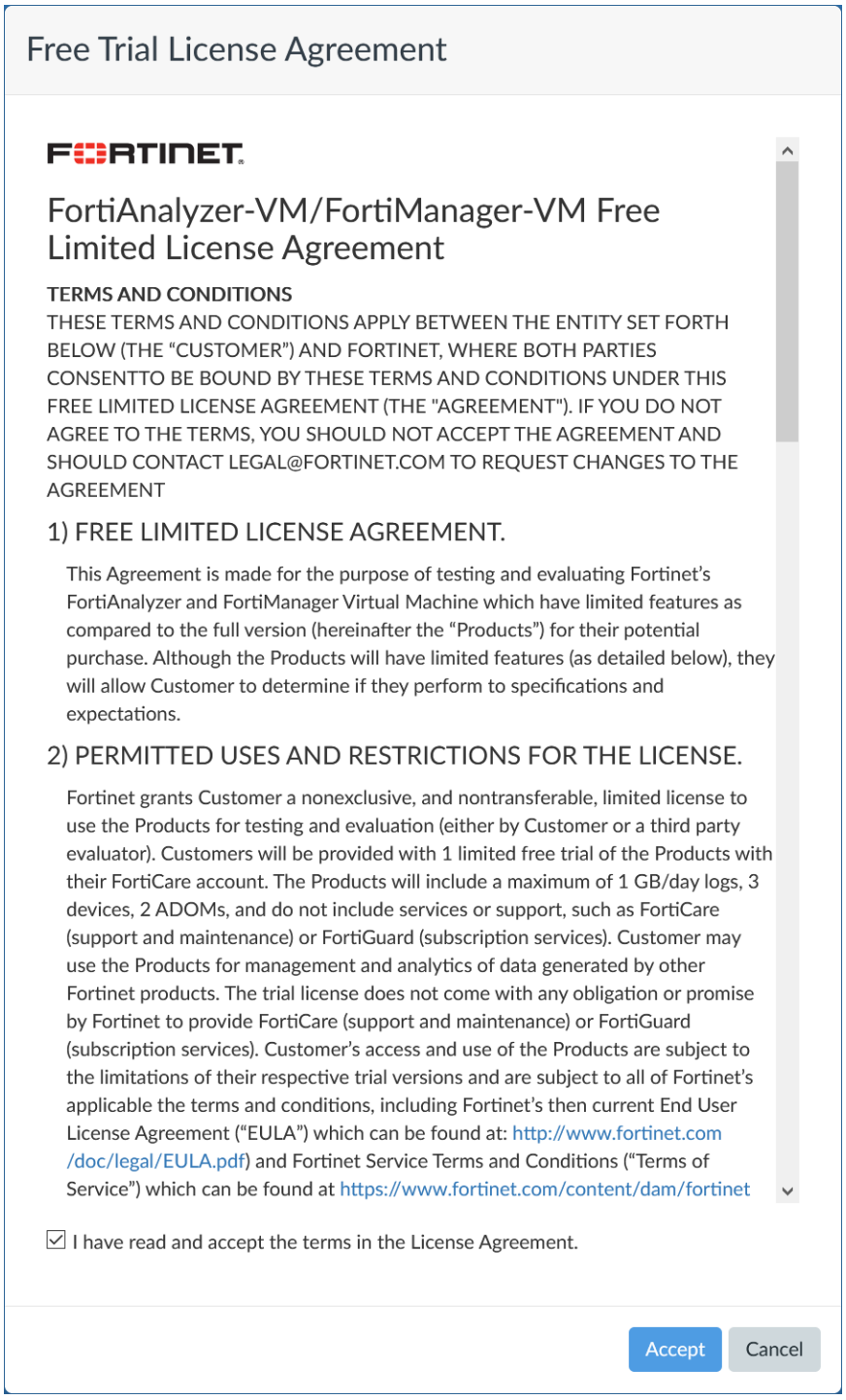
You can use the FortiAnalyzer GUI to request and activate a trial license for a FortiAnalyzer VM.

To request and activate a trial license:

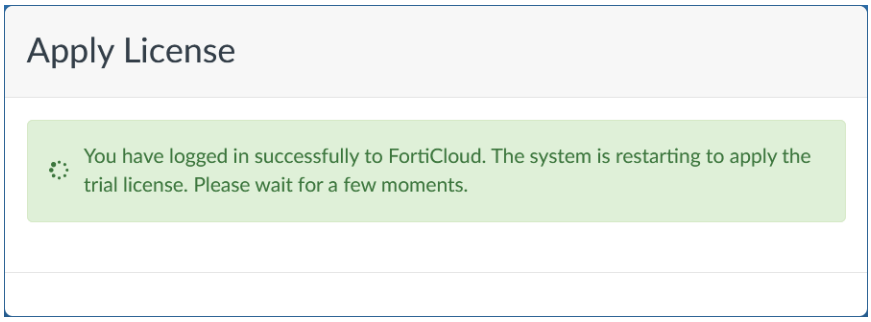
1. In a browser, access the IP address for the FortiAnalyzer GUI.
   The login dialog box is displayed.



2. Select *Free Trial*, and click *Login with FortiCloud*.
   If you do not have a FortiCloud account, click *Register with FortiCloud* to create one.
   The *Free Trial License Agreement* is displayed.



3. Accept the license agreement:
   a. Read the license agreement.
   b. Select the *I have read and accept the terms in the License Agreement* checkbox.
   c. Click *Accept*.
      The license is applied, and you are logged in to FortiAnalyzer.



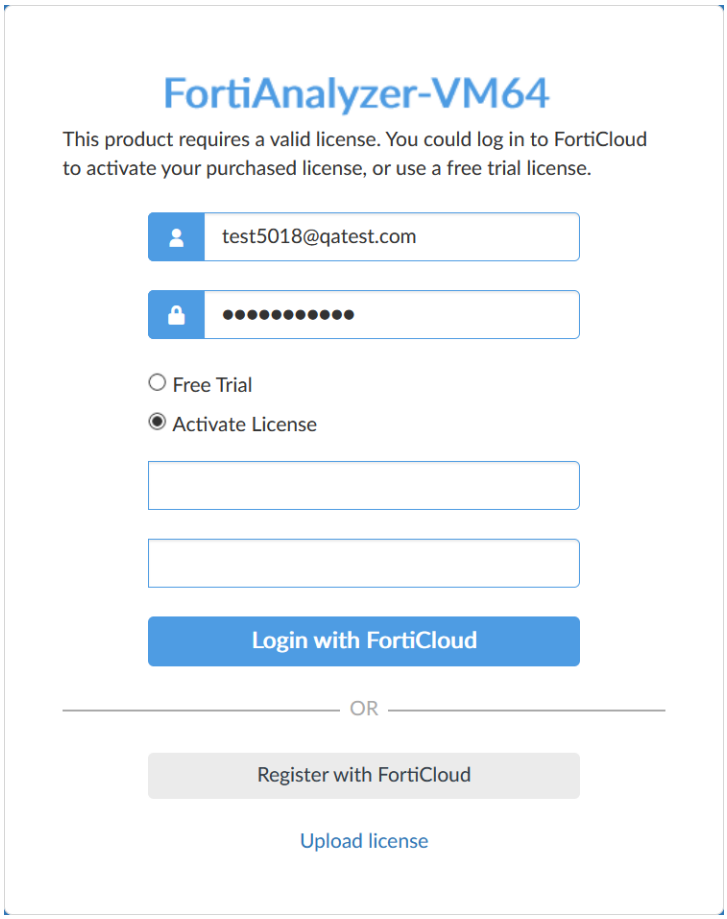
4. Go to *System Settings* > *Dashboard* > *License Information* widget.
   The *VM License* option displays *Trial License*.

Activating a new license

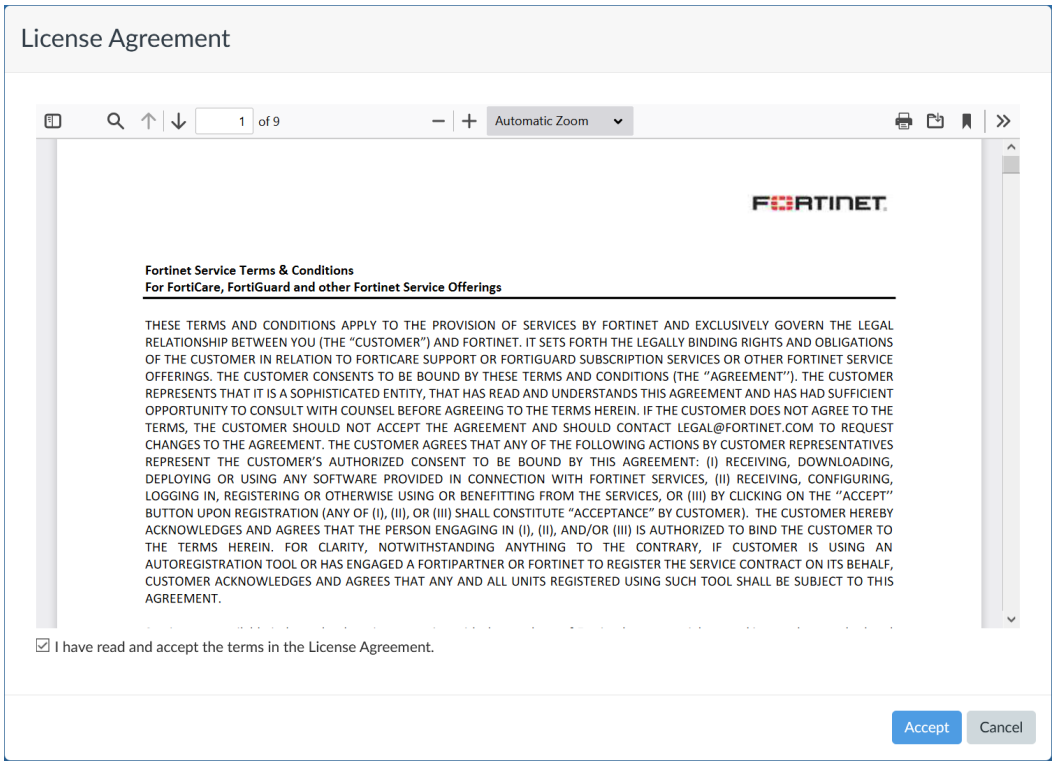
You can use the FortiAnalyzer GUI to activate a new license for virtual machines. Licenses for VM-S subscriptions and perpetual subscriptions are supported.

To activate a new license:

1. In a browser, access the IP address for the FortiAnalyzer GUI.
   The login dialog box is displayed.



2. Select *Activate License*, enter your license key, and click *Login with FortiCloud*.
   The *License Agreement* is displayed.



3. Accept the license agreement:
   a. Read the license agreement.
   b. Select the *I have read and accept the terms in the License Agreement* checkbox.
   c. Click *Accept*.
      The license is applied, and you are logged in to FortiAnalyzer.
4. Go to *System Settings* > *Dashboard* > *License Information* widget.
   The *VM License* option displays *Valid*.

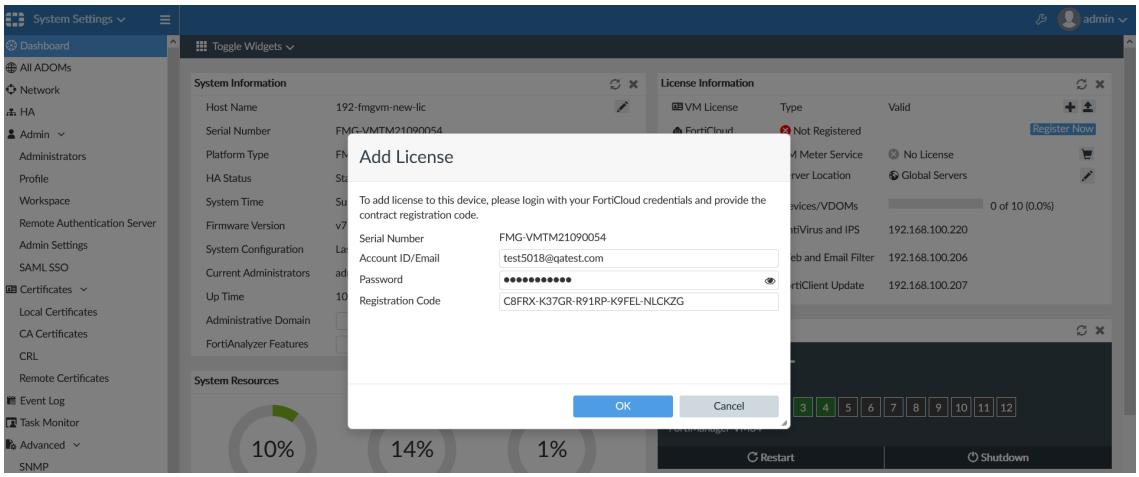
Activating an add-on license

You can use the FortiAnalyzer GUI to activate an add-on license for a VM-S subscription or a perpetual subscription.

In the following example, the FortiManager VM has a base license, and you want to apply an add-on perpetual license named *1000UG*.

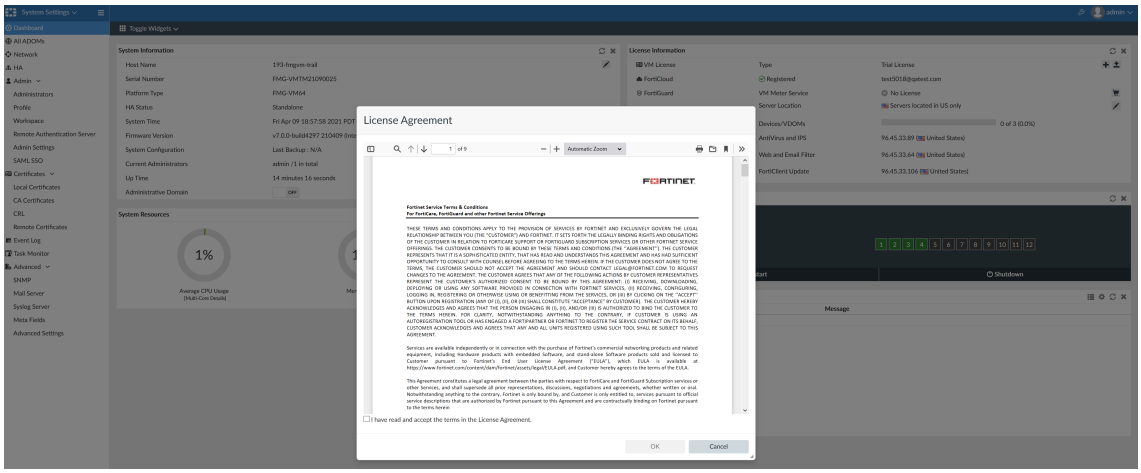
To activate an add-on license:

1. Log in to FortiAnalyzer, and go to *System Settings* > *Dashboard*.
2. In the *License Information* widget, beside the *VM License* option, click the *Add License* button.
   The *Add License* dialog box is displayed.



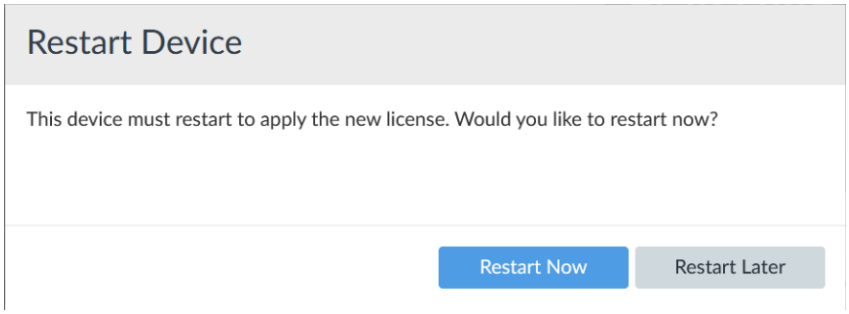
3. Complete the following options, and click *OK*:
   a. In the *Account ID/Email* box, type the email for your FortiCloud account.
   b. In the *Password* box, type the password for your FortiCloud account.
   c. In the *Registration Code* box, enter the contract registration code for the add-on license.

   The *License Agreement* is displayed.

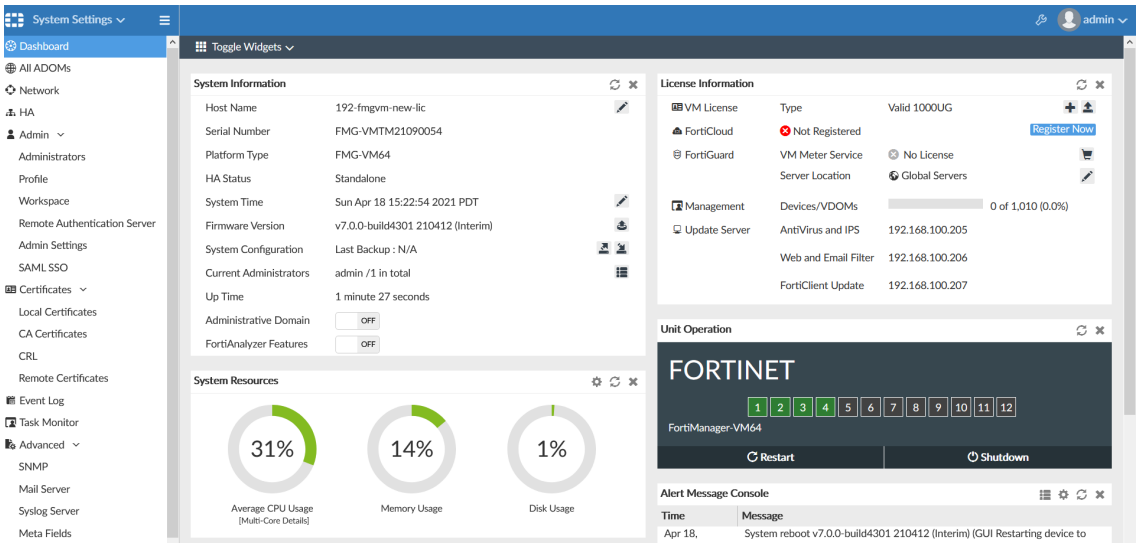


4. Accept the license agreement:
   a. Read the license agreement.
   b. Select the *I have read and accept the terms in the License Agreement* checkbox.
   c. Click *OK*.

   The *Restart Device* dialog box is displayed.



5. Click *Restart Now* to apply the license.
   FortiAnalyzer restarts, and the license is applied.
6. Go to *System Settings* > *Dashboard* > *License Information* widget.
   The *VM License* option displays *Valid 1000UG*.



FortiAnalyzer Federation

FortiAnalyzer 7.0.0 includes support for FortiAnalyzer Federation.

Configuring a FortiAnalyzer in supervisor mode provides an aggregated view of the devices, events, and incidents of each member FortiAnalyzer. Each member in the federation handles workloads and generate analytics.

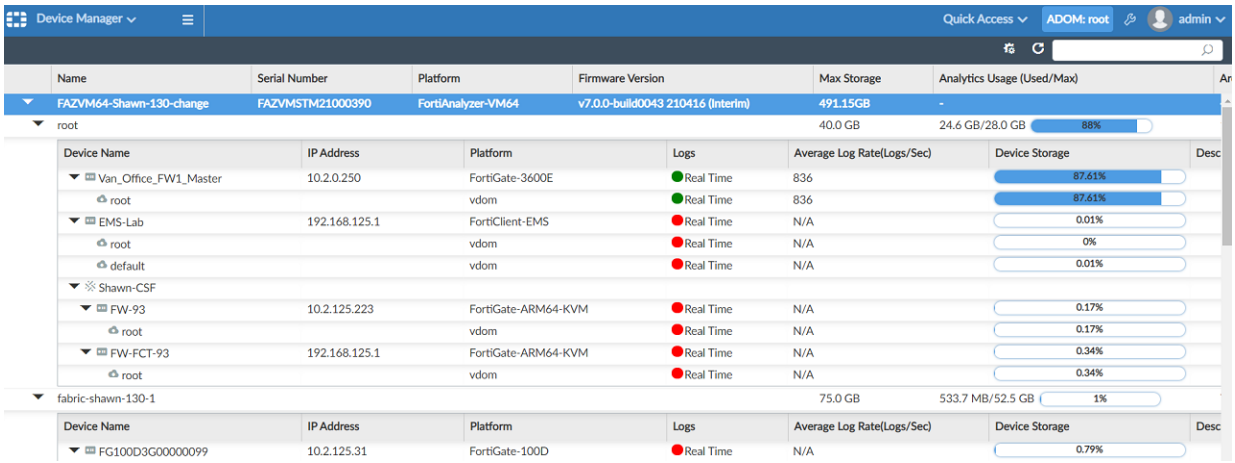
This topic includes the following:

This example scenario includes one FortiAnalyzer supervisor and three FortiAnalyzer members.

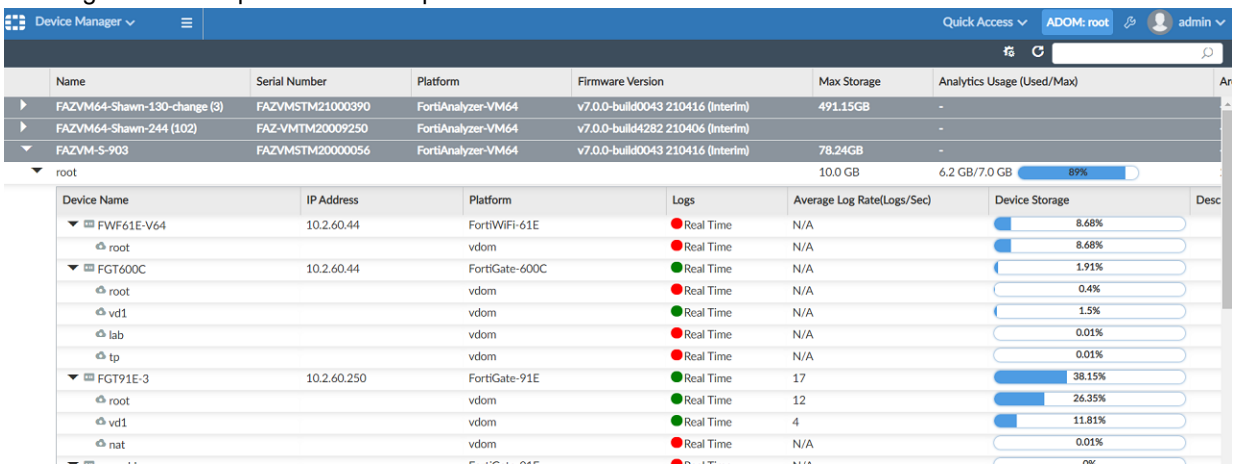
Device Manager

To view member devices in the Device Manager:

1. On the FortiAnalyzer Federation supervisor, go to *Device Manager*.
   The *Device Manager* lists all authorized member FortiAnalyzer device information as well as each member's registered devices and ADOMs.



Each member FortiAnalyzer's tree can be expanded and collapsed. When member's device status and information is changed it will be updated on the supervisor in real-time.



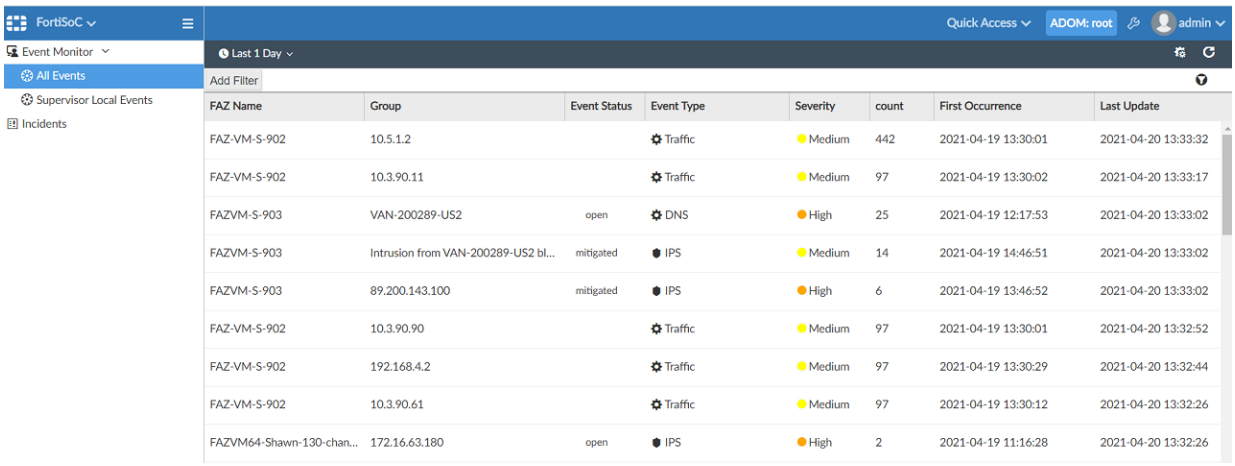
FortiSoC

FortiSoC includes the *Event Monitor* and *Incidents* panes.

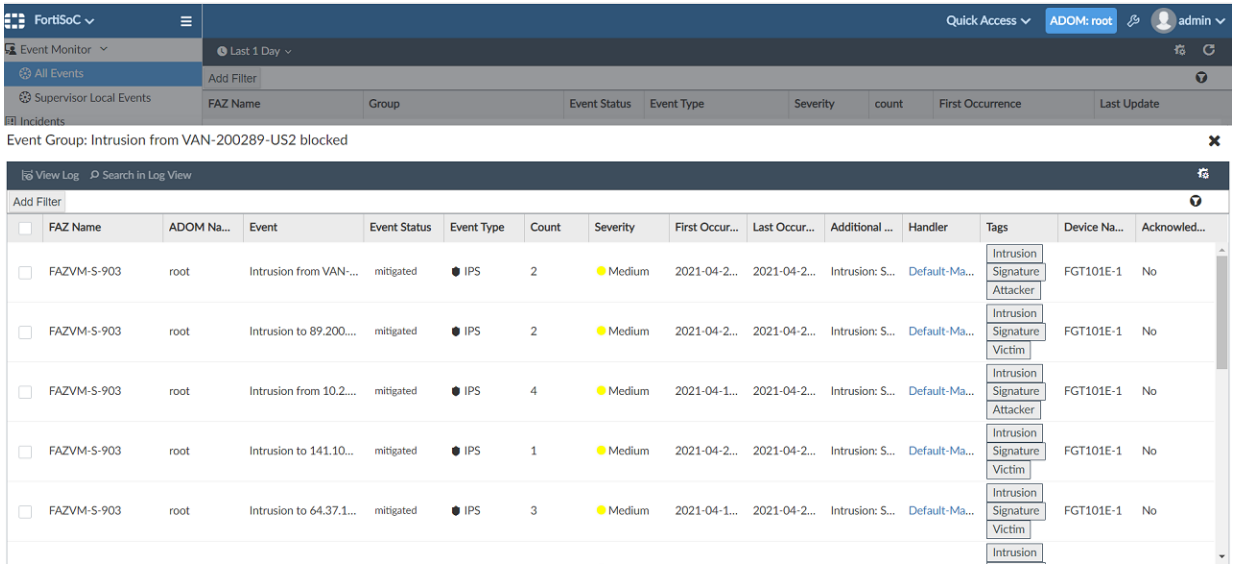
Event Monitor

To view events from members in Event Monitor:

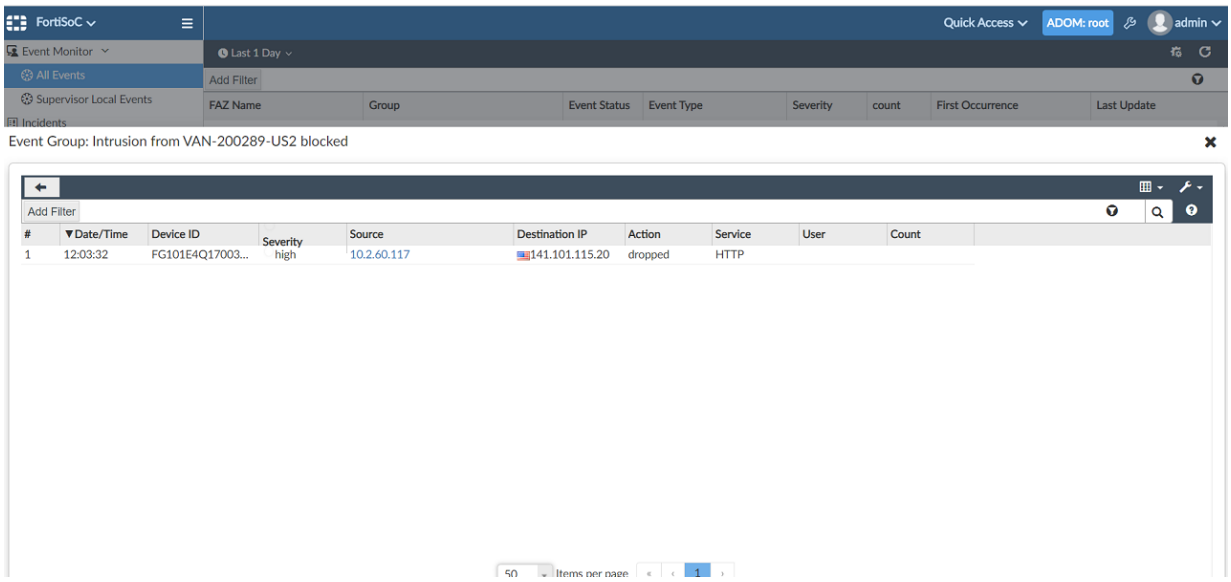
1. On the FortiAnalyzer Federation supervisor, go to *FortiSoC* > *Event Monitor* > *All Events*.
   All events from members are synced to the supervisor and are organized in event groups with different time ranges. The default view lists event groups from the last day.



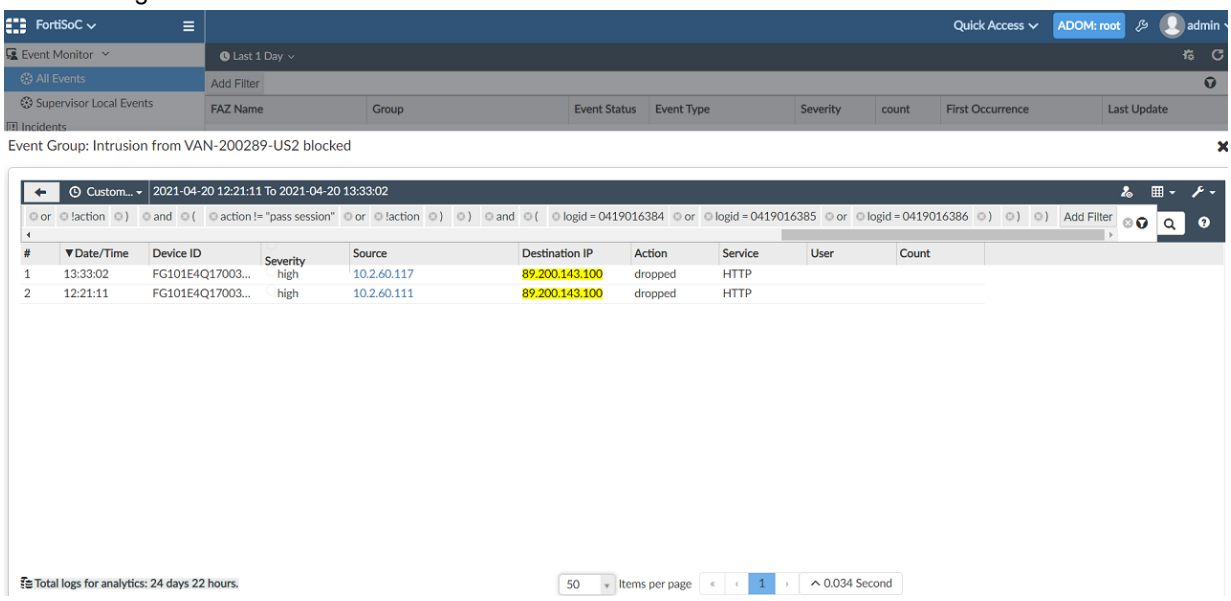
2. Click an event group to view associated events. You can drilldown to check event details.



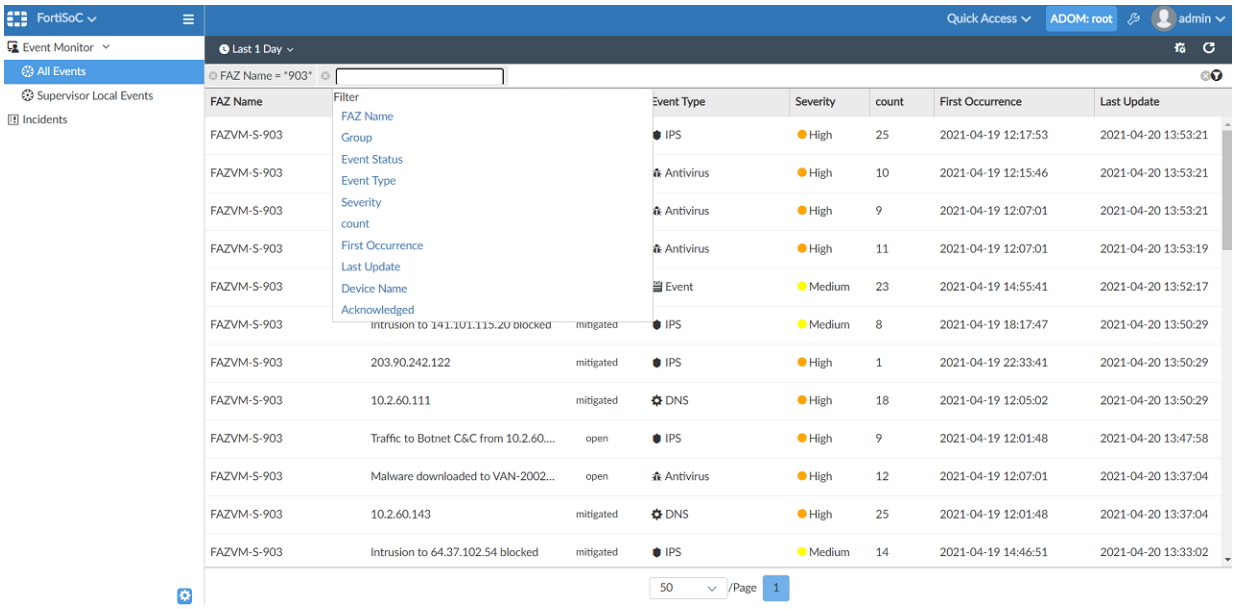
3. Select an event and click *View Log* or *Search in Log View*.
   - View logs to downstream members:



   - Search in log view from downstream members:



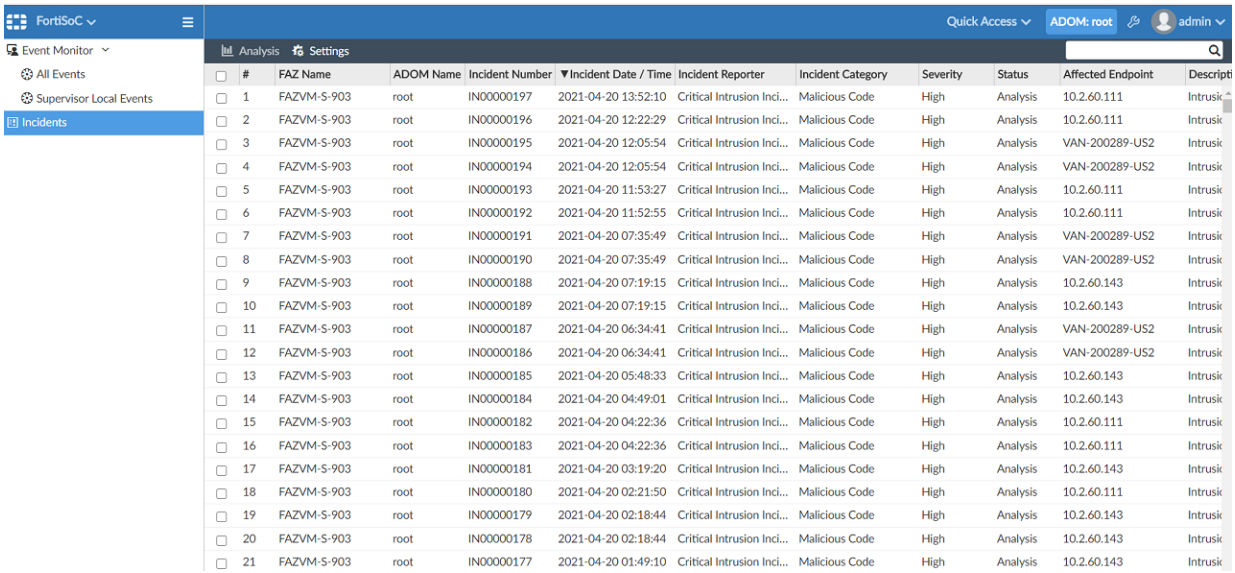
4. Add filters to narrow results, including filters for the FortiAnalyzer member name and group.



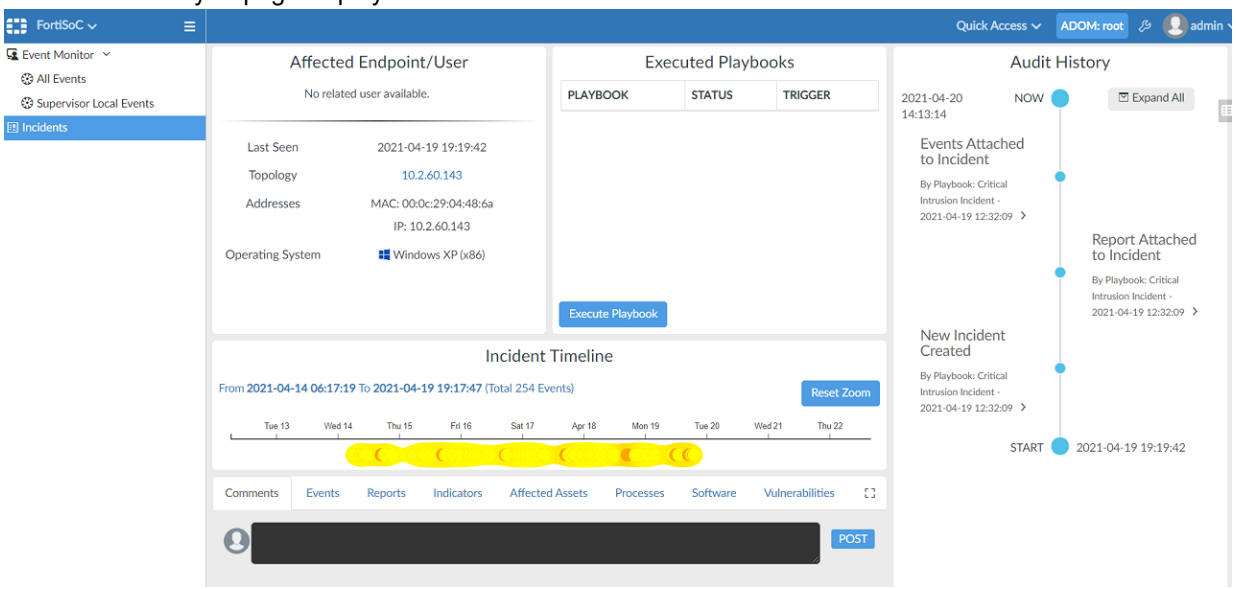
Incidents

To view incidents created on members:

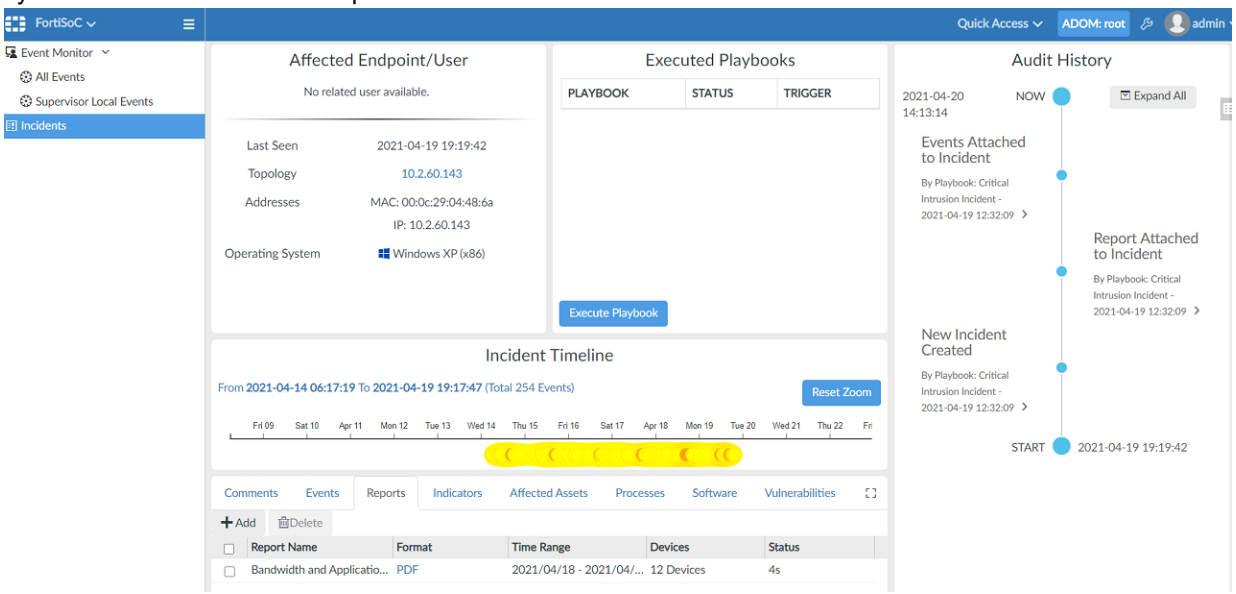
1. On the FortiAnalyzer Federation supervisor, go to *FortiSoC* > *Incidents*.
   All incidents raised on members can be synced to the supervisor when the member connects to the supervisor. Newly generated events are synced in real-time and updated on the supervisor.



2. Double-click on an incident to view the incident analysis page.
   The incident analysis page displays detailed incident information.



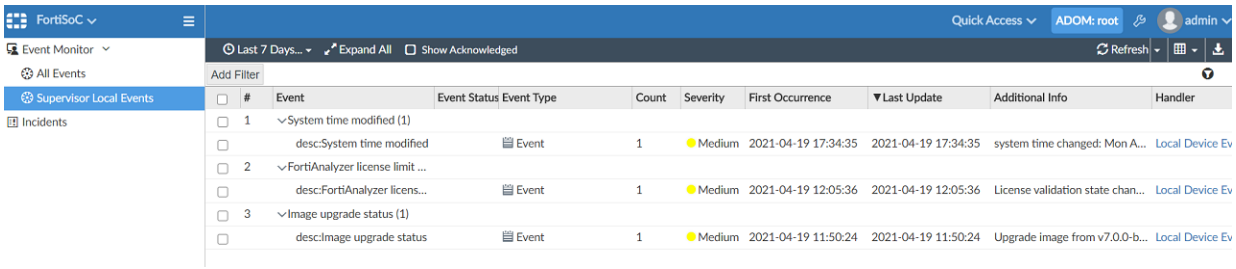
3. Check each attachment in the incident analysis page (Events, Reports, Affected Assets, etc). Attachments are synced from members to the supervisor.



Supervisor Local Events

To view supervisor local events:

1. On the FortiAnalyzer Federation supervisor, go to *FortiSoC > Event Monitor > Supervisor Local Events*.
   Local events from the supervisor are displayed.



Configure FortiAnalyzer Federation in the CLI

To configure a FortiAnalyzer Federation supervisor:

1. In the supervisor CLI, enable soc-fabric communication:
```
config system interface
   edit port1
      set allowaccess soc-fabric
```
2. Enter the following commands to configure the supervisor:
```
config system soc-fabric
set status enable
set role supervisor
set name <create the FortiAnalyzer Federation name>
set psk <create the FortiAnalyzer Federation password>
set port 6443 (set the communication port if not using the default value)
set secure-connection enable
```

Multiple FortiAnalyzer devices can be configured as members. Each FortiAnalyzer in Analyzer mode must be individually configured as a member to participate in the FortiAnalyzer federation.

To configure a FortiAnalyzer Federation member:

1. In the member CLI, enable soc-fabric communication:
```
config system interface
   edit port1
      set allowaccess soc-fabric
```
2. Enter the following commands to configure the member:
```
config system soc-fabric
   set status enable
   set role member
   set name <enter the FortiAnalyzer Federation name>
   set psk <enter the FortiAnalyzer Federation auth password>
   set supervisor ip <enter the IP/FNDN of the supervisor>
   set port 6443 <set the communication port if not using the default one>
   set secure-connection enable
```

Limitations

- FortiAnalyzer Federation supports the creation of incidents, event handlers, and events on members with centralizing viewing from the supervisor.
- FortiAnalyzer Federation supports log analysis, including *LogView* and *Reports*, on FortiAnalyzer Federation members.

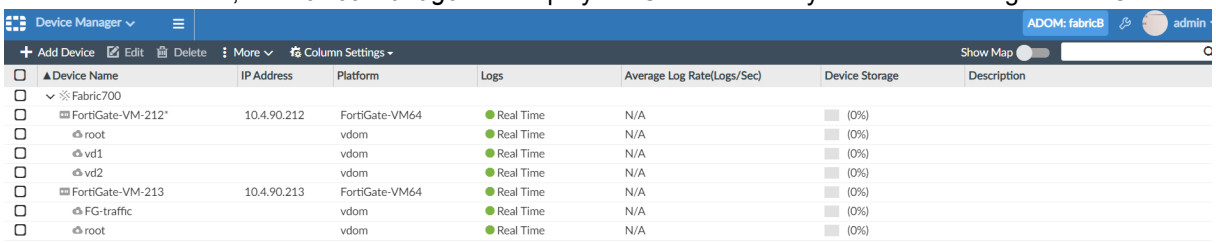
- Incidents on the FortiAnalyzer Federation supervisor are available in read-only mode.
- FortiAnalyzers configured in high availability (HA) mode can join the FortiAnalyzer Federation as members. HA is not supported for FortiAnalyzer Federation supervisors.
- All FortiAnalyzer Federation members must be configured with the same timezone settings as the supervisor.

CSF support for multiple VDOMs

Multiple VDOMs can now form a Security Fabric Cluster.

To view multiple VDOMs in a CSF on FortiAnalyzer:

1. In the FortiAnalyzer *Device Manager*, add a FortiGate running 7.0.0 which has enabled Multi VDOM mode in an ADOM.
   After a few moments, the *Device Manager* will display the Central Security Fabric with configured VDOMs.

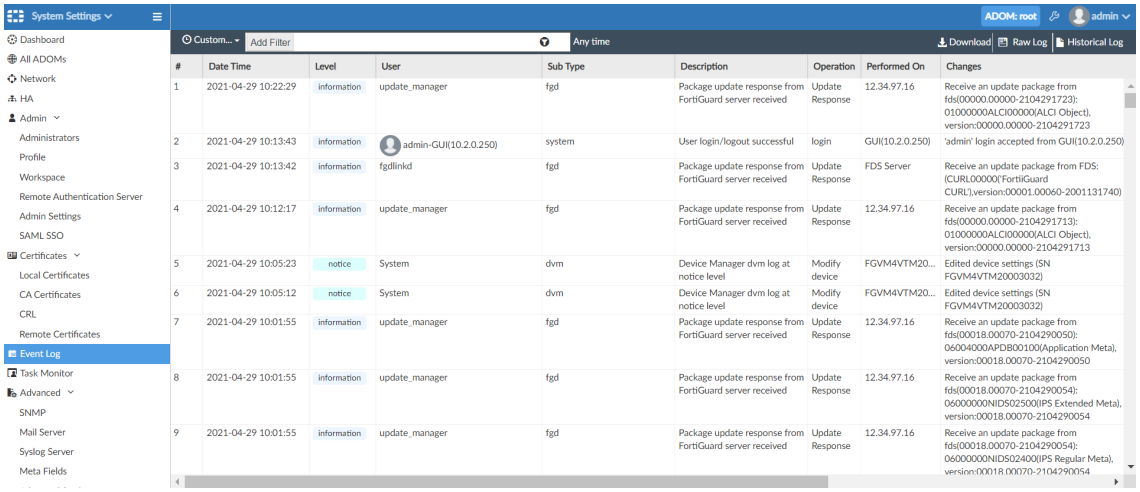


Event log easier to read - 7.0.1

The FortiAnalyzer event log includes the following new columns to make messages easier to read:

- *Operation*
- *Performed On*
- *Changes*

Go to *System Settings* > *Event* log to view the new columns:



www.fortinet.com